Dominion LX

ユーザ ガイド
リリース **2.4.5**

Copyright © 2011 Raritan, Inc.
LX-v2.4.5-0A-J
2011 年 10 月
255-80-8009-00

このドキュメントには著作権によって保護されている所有者情報が含まれています。無断で転載することは、禁じられており、このドキュメントのどの部分も Raritan, Inc.（Raritan 社）より事前に書面による承諾を得ることなく複写、複製、他の言語へ翻訳することはできません。

© Copyright 2011 Raritan, Inc.、CommandCenter®、Dominion®、Paragon®、Raritan 社のロゴは、Raritan, Inc. の商標または登録商標です。無断で転載することは、禁じられています。Java® は Sun Microsystems, Inc. の登録商標、Internet Explorer® は Microsoft Corporation の登録商標です。また、Netscape® および Netscape Navigator® は Netscape Communication Corporation の登録商標です。その他すべての商標または登録商標は、その所有会社に帰属します。

FCC 情報

この装置は FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが試験により証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設けられています。この装置は、無線周波数を生成、利用、放射する可能性があるので、指示に従った設置および使用をしないと、無線通信への干渉を招く恐れがあります。この装置を居住環境で操作すると、干渉を招く場合があります。

VCCI 情報 (日本)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が関与しない範囲での使用や、通常の運用条件以外での使用による製品の故障については、Raritan 社は一切責任を負いかねます。

CE c UL us LISTED 1F61 I.T.E.

ラック マウントの安全上のガイドライン

ラック マウントが必要なラリタン製品を使用する場合、以下のことに注意してください。

- 閉め切ったラック環境では、室温より高くなる場合があります。装置で指定された最高動作温度を超えないようにしてください。**仕様**を参照してください。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機械的に安定して搭載されるように注意してマウントしてください。
- 回路に過大電流が流れないよう、装置を電源に接続する際は注意してください。
- 特に、電源タップ（直接接続を除く）など電力供給をはじめとするすべての装置を分岐回路に正しく接地してください。

目次

Ch 1 はじめに

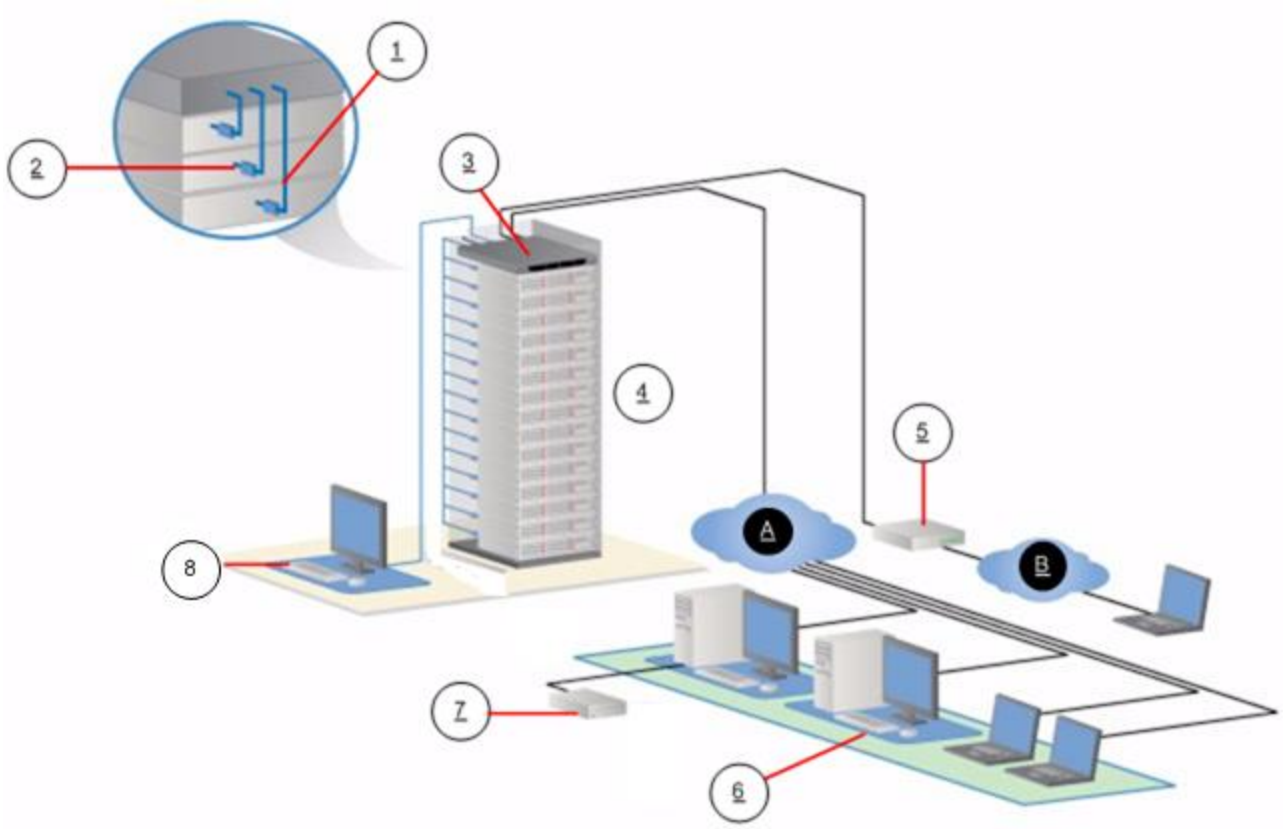
この章の内容

LX の概要

LX® KVM-over-IP スイッチを使用すると、独立したローカル ポートで 1、2 名のリモート ユーザが、BIOS レベルで最大 16 台のサーバのアクセスや制御を行うことができます。カスケード接続機能を実装すると、ユーザは、1 か所のコンソールから最大 256 台のコンピュータを容易に管理できます。こうしたアプライアンス、特に中小企業（SMB）向けに設計されたアプライアンスにより、どこからでも経済的なリモート アクセスや信頼性の高い効率的なサーバ管理を行うことができ、最小限の初期投資で安価に拡張できます。

LX は、Raritan のユニバーサル仮想メディア™ を標準装備しており、CD、DVD、USB、内蔵ドライブ、リモート ドライブなどのさまざまなデバイスをローカルにマウントしてリモートで管理できるようになるので、移動する必要がなくなります。クリアで鮮明な表示を得るために、最新のアーキテクチャ プラットフォームでは、ローカル アクセスとリモート アクセスの両方に対して高画質（HD）1920x1080 のリモート画面解像度および一般的な最新のブラウザベースの GUI をサポートしているので、ほとんどトレーニングの必要がなく、ローカルでの作業と同等の生産性が得られ、すべての IT リソースを効率的に利用できます。サーバには、Windows®、Linux®、Sun®、または Macintosh® から主要なブラウザを介してアクセスするか、クライアント ライセンス料金なしにスタンドアロンでアクセスすることができます。

ケーブル バンドル オプションにより、SMB の IT スタッフは、後から追加する機能のオプションを維持しながら現在の初期投資を最小限に抑えることができます。



図の説明			
1	Cat5 ケーブル	6	リモート（ネットワーク）アクセス
2	コンピュータ インタフェース モジュール（CIM）	7	ローカル アクセス
3	LX	A	IP LAN/WAN
4	リモート KVM およびシリアル デバイス	B	PSTN
5	モデム		

LX の写真

LX 108


Raritan
Dominion LX-116
RESET
LAN
MODEM

LX 116


Raritan
Dominion LX-216
RESET
LAN
MODEM

LX 216

Raritan.

パッケージの内容

LX は、標準 1U 19 インチ ラックマウント シャーシに搭載される、完全に構成されたスタンドアロン製品として出荷されます。各 LX デバイスは、以下の内容で出荷されます。

数量	品目
1	LX デバイス
1	ラックマウント キット
1	AC 電源コード
1	LX クイック セットアップ ガイド
1	アプリケーション ノート
1	保証書

LX のクライアント アプリケーション

LX で使用できるクライアント アプリケーションは、次のとおりです。

製品	使用可能				
	MPC	RRC	VKC	RSC	AKC
LX 2.4.5 以降	✓		✓		✓

クライアント アプリケーションの詳細については、『KVM and Serial Access Clients User Guide』を参照してください。このガイドの「*ターゲット サーバの使用 『39*p. 』」セクションも参照してください。LX でのクライアントの使用に関する情報が記載されています。

注: MPC および VKC を使用するには、Java™ Runtime Environment (JRE™) が必要です。AKC は .NET ベースです。

ハードウェア

- KVM-over-IP リモート アクセスの統合
- 8 サーバ ポート モデルと 16 サーバ ポート モデル
- 最大 2 つのビデオ チャネルを搭載し、最大 2 人のユーザが同時に LX に接続可能
- マルチ ユーザ機能 (1/2 リモート ユーザ、1 ローカル ユーザ)
- UTP (Cat5/5e/6) ケーブルを使用したサーバへの配線
- Ethernet ポート (10/100/1000 LAN)
- 現場でアップグレード可能
- ラック内アクセス用ローカル ユーザ ポート
  - サポートされている USB デバイス用の USB 2.0 ポート (背面に 3 基)
  - リモート ユーザ アクセスと同時に操作可能
  - 管理用のローカル グラフィカル ユーザ インタフェース (GUI)
- モデム サポート
- デバイス ステータス、起動、およびファームウェア アップグレード用の前面と背面の LED インジケータ
- ハードウェア リセット ボタン
- 外付けモデムに接続するためのシリアル ポート
- 19 インチ ラックマウント対応 (ブラケット付属)

ソフトウェア

- Windows®、Mac®、Linux® の各環境で仮想メディアをサポート (D2CIM-VUSB および D2CIM-DVUSB CIM により提供)
- 設定可能なスキャン セット内でターゲットをポート スキャンしサムネイル表示
- ずれないマウス機能 (D2CIM-VUSB CIM および D2CIM-DVUSB CIM により提供)
- プラグ アンド プレイ
- Web ベースのアクセスと管理
- わかりやすいグラフィカル ユーザ インタフェース (GUI)
- すべての KVM 信号を 256 ビット暗号化 (ビデオや仮想メディアを含む)
- LDAP、Active Directory®、RADIUS、または内部機能による認証および認可
- DHCP または静的な IP アドレスの指定
- SNMP および Syslog 管理
- IPv4 および IPv6 のサポート
- LX および汎用カスケード接続

LX ヘルプ

LX ヘルプでは、LX のインストール、セットアップ、および設定の方法に関する情報を確認できます。また、ターゲット サーバに対するアクセス、仮想メディアの使用、ユーザおよびセキュリティの管理、LX の保守と診断に関する情報も提供します。

現在のリリースに関する重要な情報について LX リリースノートを参照してから、LX を使用してください。

PDF バージョンのヘルプは、Raritan の Web サイトの [Firmware and Documentation] ページからダウンロードできます。最新のユーザ ガイドが利用できるかどうかを Raritan の Web サイトで確認することをお勧めします。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

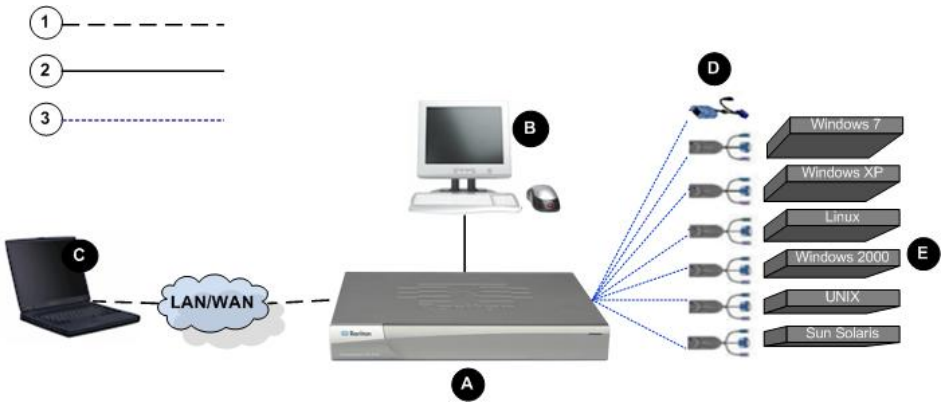
関連文書

LX ヘルプには、LX クイック セットアップ ガイドが付属しています。これは、*Raritan の Web サイト*『*http://www.raritan.com/support/firmware-and-documentation*see 』の [Firmware and Documentation] ページにあります。

LX で使用するクライアント アプリケーションのインストールの要件および手順についても、Raritan の Web サイトにある『KVM and Serial Access Clients Guide』を参照してください。該当する場合は、LX で使用される特定のクライアント機能がこのヘルプに掲載されます。

用語

ヘルプでは、LX の代表的なコンポーネントに以下の用語を使用しています。



図の説明	
1	TCP/IP 追加した IPv4 または IPv6
2	KVM (キーボード、ビデオ、マウス)
3	UTP ケーブル (Cat5/5e/6)
A	LX
B	ローカル アクセス コンソール ローカル ユーザ: ターゲット サーバを (ネットワーク経由ではなく直接ラック内で) 制御するために LX に直接接続された、(キーボード、マウス、マルチシンク VGA モニタで構成される) オプションのユーザ コンソール。
C	リモート PC LX に接続している KVM ターゲット サーバへのアクセスとその制御に使用する、ネットワークに接続したコンピュータ。
D	CIM 各ターゲット サーバに接続するドングル。サポートされているすべてのオペレーティング システムに対して使用できます。
E	ターゲット サーバ KVM ターゲット サーバ: LX を介してリモート アクセスされる、ビデオ カードとユーザ インタフェース (例: Windows®、Linux®、Solaris™) を備えたサーバ。

サポートされているオペレーティング システムおよび CIM については、「サポートされている CIM およびオペレーティング システム －LX」を参照してください。

Ch 2 インストールと設定

この章の内容

概要

このセクションでは、インストール手順の概要を説明します。それぞれの手順については、この章の後のセクションで詳しく説明します。

▶ **LX をインストールおよび設定するには、以下の手順に従います。**

- *手順 1: KVM ターゲット サーバの設定* 『13p. 』
- *手順 2: ネットワーク ファイアウォールの設定* 『27p. 』
- *手順 3: 装置の接続* 『28p. 』
- *手順 4: LX* 『30p. の"*手順 4: LX の設定*"参照 』 の設定
- *手順 5: LX リモート コンソールの起動* 『36p. 』
- *手順 6: キーボード言語の設定 (オプション)* 『37p. 』
- *手順 7: カスケード接続の設定 (オプション)* 『38p. 』

このセクションには、必要なデフォルトのログイン情報も含まれます。この情報には、特にデフォルト IP アドレス、ユーザ名、およびパスワードがあります。「*デフォルトのログイン情報* 『12p. 』」を参照してください。

デフォルトのログイン情報

デフォルト設定	値
ユーザ名	デフォルトのユーザ名は admin です。このユーザは、管理者特権を有します。
パスワード	デフォルトのパスワードは raritan です。 パスワードは大文字と小文字が区別されるため、大文字と小文字は作成したとおりに正確に入力する必要があります。たとえば、デフォルトのパスワード raritan は、すべて小文字で入力する必要があります。 LX を初めて起動したときは、デフォルトのパスワードを変更する必要があります。
IP アドレス	LX の出荷時には、デフォルトの IP アドレス

デフォルト設定	値
	(192.168.0.192) が設定されています。

重要: バックアップと事業の継続性のためには、バックアップ管理者用のユーザ名およびパスワードを作成し、その情報を安全な場所に保管しておくことを強くお勧めします。

入門

手順 1: KVM ターゲット サーバの設定

KVM ターゲット サーバとは、LX を介してアクセスおよび制御するコンピュータのことです。最適なパフォーマンスを確保するために、LX をインストールする前に、すべての KVM ターゲット サーバを設定します。この設定は、KVM ターゲット サーバのみに適用されます。LX のリモート アクセスに使用されるクライアント ワークステーション (リモート PC) には適用されません。

デスクトップの背景

帯域幅効率とビデオ パフォーマンスを最適化するために、できるだけ単色の背景を使用してください。写真や複雑な階調を持つ背景を使用すると、パフォーマンスが低下する場合があります。

サポートされている画面解像度

各ターゲット サーバの画面解像度とリフレッシュ レートが LX でサポートされているかどうか、および、映像信号がノンインタレース方式であるかどうかを確認してください。

画面解像度とケーブル長は、マウスを同期させるうえで重要な要素です。「*ターゲット サーバとの接続距離および画面解像度* 『*210*p. 』」を参照してください。

LX でサポートされている画面解像度は次のとおりです。

解像度	
640x350、70Hz	1024x768、85Hz
640x350、85Hz	1024x768、75Hz
640x400、56Hz	1024x768、90Hz
640x400、84Hz	1024x768、100Hz

解像度	
640x400、85Hz	1152x864、60Hz
640x480、60Hz	1152x864、70Hz
640x480、66.6Hz	1152x864、75Hz
640x480、72Hz	1152x864、85Hz
640x480、75Hz	1152x870、75.1Hz
640x480、85Hz	1152x900、66Hz
720x400、70Hz	1152x900、76Hz
720x400、84Hz	1280x720、60Hz
720x400、85Hz	1280x960、60Hz
800x600、56Hz	1280x960、85Hz
800x600、60Hz	1280x1024、60Hz
800x600、70Hz	1280x1024、75Hz
800x600、72Hz	1280x1024、85Hz
800x600、75Hz	1360x768、60Hz
800x600、85Hz	1366x768、60Hz
800x600、90Hz	1368x768、60Hz
800x600、100Hz	1400x1050、60Hz
832x624、75.1Hz	1440x900、60Hz
1024x768、60Hz	1600 x 1200、60Hz
1024x768、70Hz	1680x1050、60Hz
1024x768、72Hz	1920x1080、60Hz

マウス モード

LX は、ずれないマウス モード™、インテリジェント マウス モード、および標準マウス モードで動作します。

ずれないマウス モードの場合は、マウス パラメータを変更する必要はありません。ただし、D2CIM-VUSB または D2CIM-DVUSB が必要です。標準マウス モードとインテリジェント マウス モードの場合、マウス パラメータを特定の値に設定する必要があります。マウス設定は、ターゲットのオペレーティング システムによって異なります。詳細については、使用するオペレーティング システムのマニュアルを参照してください。

インテリジェント マウス モードは、ほとんどの Windows プラットフォームで正常に機能しますが、ターゲット上でアクティブ デスクトップが設定されている場合は、予測できない結果を生じることがあります。インテリジェント マウス モードではアニメーション カーソルは使用しないでください。

Windows XP、Windows 2003、および Windows 2008 の設定

▶ **Microsoft® Windows XP® オペレーティング システムを実行している KVM ターゲット サーバを設定するには、Windows 2003® オペレーティング システムまたは Windows 2008® オペレーティング システムで、以下の操作を行います。**

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[マウス] の順に選択します。
   b. [ポインタ オプション] タブをクリックします。
   c. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [動作] のオプションを無効にします。
      - [OK] をクリックします。

注: ターゲット サーバで Windows 2003 を実行している場合に、KVM を介してサーバにアクセスし、次に挙げるアクションのいずれかを実行すると、以前有効になっていたマウスの同期が失われる可能性があります。同期を再度有効にするには、クライアントで [マウス] メニューの [マウスの同期] コマンドを選択する必要があります。これが発生する可能性があるアクションを以下に示します。

- テキスト エディタを開く。

- Windows の [コントロール パネル] から [マウスのプロパティ]、[キーボードのプロパティ]、および [電話とモデムのオプション] にアクセスする。

---

2. アニメーション効果を無効にします。
   a. [コントロール パネル] の [画面] オプションを選択します。
   b. [デザイン] タブをクリックします。
   c. [効果] をクリックします。
   d. [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにします。
   e. [OK] をクリックします。
3. [コントロール パネル] を閉じます。

注: Windows XP、Windows 2000、または Windows 2008 を実行している KVM ターゲット サーバの場合、LX を介したリモート接続用に、専用のユーザ名を作成することが可能です。これにより、ターゲット サーバのマウス ポインタの速度や加速を LX 接続用に遅く設定できます。

Windows XP、2000、および 2008 のログイン ページでは、マウスのパラメータが、最適な LX パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。この結果、これらの画面ではマウスの同期は最適ではありません。

注: Windows KVM ターゲット サーバのレジストリを調整してもかまわない場合のみ、次の操作を行ってください。Windows レジストリ エディタを使って次の設定を変更することにより、ログイン ページで LX のマウスの同期を改善することができます。HKey_USERS¥.DEFAULT¥Control Panel¥Mouse:> MouseSpeed = 0、MouseThreshold 1=0、MouseThreshold 2=0。

Windows 7 および Windows Vista の設定

Windows Vista® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. [スタート]、[設定]、[コントロール パネル]、[マウス] の順に選択します。
   b. 左側のナビゲーション パネルから [システムの詳細設定] を選択します。[システムのプロパティ] ダイアログ ボックスが表示されます。
   c. [ポインタ オプション] タブをクリックします。
   d. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [OK] をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. [コントロール パネル] の [システム] オプションを選択します。

b. [パフォーマンス情報] を選択し、[ツール]、[詳細ツール]、[調整] の順に選択し、Windows の外観とパフォーマンスを調整します。
c. [詳細設定] タブをクリックします。
d. [パフォーマンス] グループの [設定] をクリックして、[パフォーマンス オプション] ダイアログ ボックスを開きます。
e. [カスタム] オプションで、以下のチェック ボックスをオフにします。

- アニメーション関連のオプション:
  - [Windows 内のアニメーション コントロールと要素]
  - [ウィンドウを最大化や最小化するときにアニメーションで表示する]
- フェード関連のオプション:
  - [メニューをフェードまたはスライドして表示する]
  - [ヒントをフェードまたはスライドで表示する]
  - [メニュー項目をクリック後にフェード アウトする]

3. [OK] をクリックして、[コントロール パネル] を閉じます。

Windows 7® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[ハードウェアとサウンド]、[マウス] の順に選択します。
   b. [ポインタ オプション] タブをクリックします。
   c. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [OK] をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. [コントロール パネル]、[システムとセキュリティ] を選択します。
   b. [システム] を選択し、左側のナビゲーション パネルから [システムの詳細設定] を選択します。[システムのプロパティ] ダイアログ ボックスが表示されます。
   c. [詳細設定] タブをクリックします。
   d. [パフォーマンス] グループの [設定] ボタンをクリックして、[パフォーマンス オプション] ダイアログ ボックスを開きます。
   e. [カスタム] オプションで、以下のチェック ボックスをオフにします。
   - アニメーション関連のオプション:

- [Windows 内のアニメーション コントロールと要素]
- [ウィンドウを最大化や最小化するときにアニメーションで表示する]

- フェード関連のオプション:
  - [メニューをフェードまたはスライドして表示する]
  - [ヒントをフェードまたはスライドで表示する]
  - [メニュー項目をクリック後にフェード アウトする]

3. [OK] をクリックして、[コントロール パネル] を閉じます。

Windows 2000 の設定

Microsoft® Windows 2000® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[マウス] の順に選択します。
   b. [Motion] (動作) タブをクリックします。
      - アクセラレーションを [なし] に設定します。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [OK] (OK) をクリックします。
2. アニメーション効果を無効にします。
   a. [コントロール パネル] の [画面] オプションを選択します。
   b. [効果] タブをクリックします。
      - [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにします。
3. [OK] をクリックして、[コントロール パネル] を閉じます。

注: Windows XP、Windows 2000、または Windows 2008 を実行している KVM ターゲット サーバの場合、LX を介したリモート接続用に、専用のユーザ名を作成することが可能です。これにより、ターゲット サーバのマウス ポインタの速度や加速を LX 接続用に遅く設定できます。

Windows XP、2000、および 2008 のログイン ページでは、マウスのパラメータが、最適な LX パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。この結果、これらの画面ではマウスの同期は最適ではありません。

注: Windows KVM ターゲット サーバのレジストリを調整してもかまわない場合のみ、次の操作を行ってください。Windows レジストリ エディタを使って次の設定を変更することにより、ログイン ページで LX のマウスの同期を改善することができます。HKey_USERS¥.DEFAULT¥Control Panel¥Mouse:> MouseSpeed = 0、MouseThreshold 1=0、MouseThreshold 2=0。

Linux の設定 (Red Hat 9)

注: 以下の設定は、標準マウス モード専用に最適化されています。

Linux® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (グラフィカル ユーザ インタフェース)。

1. マウスの設定を行います。
   a. メイン メニュー、[Preferences] (個人設定)、[Mouse] (マウス) の順に選択します。[Mouse Preferences] (マウスの設定) ダイアログ ボックスが表示されます。
   b. [Motion] (動作) タブをクリックします。
   c. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間に設定します。
   d. [Speed] (速度) グループ内で、[Sensitivity] (感度) を低く設定します。
   e. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値を小に設定します。
   f. [Mouse Preferences] (マウスの設定) ダイアログ ボックスを閉じます。

   注: これらの手順でうまく設定できない場合は、Linux com コマンド ラインの方法で説明されているように、コマンド「xset mouse 1 1」を入力します。

2. 画面解像度を設定します。
   a. メイン メニュー、[System Settings] (システム設定)、[Display] (画面) の順に選択します。[Display Settings] (画面の設定) ダイアログ ボックスが表示されます。
   b. [Display] (画面) タブから、LX でサポートされている解像度を選択します。
   c. [Advanced] (高度) タブから、LX でサポートされている垂直走査周波数を確認します。

注: ターゲット サーバに接続している場合、ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ を押すと、XF86Config または /etc/X11/xorg.conf (使用中の X サーバ ディストリビューションに応じて決まります) で有効になっているすべての解像度が順にスクロールされ、ビデオ解像度が変更されます。

Linux を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (コマンド ライン)。

1. マウスの加速を正確に 1 に設定し、しきい値も正確に 1 に設定します。コマンド「*xset mouse 1 1*」を入力します。このコマンドは、ログイン時の実行用に設定する必要があります。

2. Linux を実行している各ターゲット サーバが、LX でサポートされている解像度を、標準 VESA 解像度および垂直走査周波数で使用していることを確認します。
3. さらに、各 Linux ターゲット サーバを、ブランキング時間が VESA の標準値の +/- 40% になるように設定する必要があります。
   a. Xfree86 設定ファイル XF86Config を表示します。
   b. テキスト エディタを使用して、LX でサポートされていない解像度をすべて無効にします。
   c. (LX でサポートされていない) 仮想デスクトップ機能を無効にします。
   d. ブランキング時間を確認します (VESA 標準の +/- 40%)。
   e. コンピュータを再起動します。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログオフし、再度ログインする必要があります。

Red Hat 9 KVM ターゲット サーバに関する注意

USB CIM が使用されているターゲット サーバで Red Hat® 9 を実行していて、キーボードやマウスに問題が発生した場合は、ここに説明する設定を試すことができます。

ヒント: これらの手順は、OS を新規にインストールした後でも実行する必要があります。

▶ USB CIM を使用している Red Hat 9 サーバを設定するには以下の手順に従います。

1. システムの設定ファイル (通常は /etc/modules.conf) を探します。
2. 任意のエディタを使用して、modules.conf ファイルの alias usb-controller 行を次のように設定します。

   alias usb-controller usb-uhci

   注: /etc/modules.conf ファイル内で usb-uhci が記述されている行が他に存在する場合は、その行を削除するかコメントアウトする必要があります。
3. ファイルを保存します。
4. 変更を有効にするために、システムをリブートします。

Linux の設定 (Red Hat 4)

注: 以下の設定は、標準マウス モード専用に最適化されています。

▶ **Linux® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (グラフィカル ユーザ インタフェース)。**

1. マウスの設定を行います。
   a. Red Hat 5 ユーザの場合は、**メイン メニュー、[Preferences] (個人設定)、[Mouse] (マウス) の順に選択します。Red Hat 4 ユーザの場合は、[System] (システム)、[Preferences] (個人設定)、[Mouse] (マウス) の順に選択します。[Mouse Preferences] (マウスの設定) ダイアログ ボックスが表示されます。**
   b. [Motion] (モーション) タブをクリックします。
   c. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間に設定します。
   d. [Speed] (速度) グループ内で、[Sensitivity] (感度) を低く設定します。
   e. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値を小に設定します。
   f. [Mouse Preferences] (マウスの設定) ダイアログ ボックスを閉じます。

   注: これらの手順でうまく設定できない場合は、Linux com コマンドラインの方法で説明されているように、コマンド「xset mouse 1 1」を入力します。

2. 画面解像度を設定します。
   a. メイン メニュー、[System Settings] (システム設定)、[Display] (画面) の順に選択します。[Display Settings] (画面の設定) ダイアログ ボックスが表示されます。
   b. [Settings] (設定) タブから、LX でサポートされている解像度を選択します。
   c. [OK] をクリックします。

注: ターゲット サーバに接続すると、ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ を押すと、XF86Config または /etc/X11/xorg.conf (使用中の X サーバ ディストリビューションに応じて決まります) で有効になっているすべての解像度が順にスクロールされ、ビデオ解像度が変更されます。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

SUSE Linux 10.1 の設定

注: SUSE Linux® ログイン プロンプトでマウスを同期しないでください。マウス カーソルを同期するには、ターゲット サーバに接続している必要があります。

▶ **マウスを設定するには、以下の手順に従います。**

1. **[デスクトップ] メニューの [コントロールセンター] を選択します。[Desktop Preferences] (デスクトップの設定) ダイアログ ボックスが表示されます。**
2. [Mouse] (マウス) をクリックします。[Mouse Preferences] (マウスの設定) ダイアログ ボックスが表示されます。
3. [Motion] (動作) タブを開きます。
4. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間位置に設定します。
5. [Speed] (速度) グループ内で、[Sensitivity] (感度) スライダを低く設定します。
6. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値スライダを小に設定します。
7. [Close] (閉じる) をクリックします。

▶ **ビデオを設定するには、以下の手順に従います。**

1. [Desktop Preferences] (デスクトップの設定) の [Graphics Card and Monitor] (グラフィックカードとモニター) を選択します。[Card and Monitor Properties] (カードとモニターのプロパティ) ダイアログ ボックスが表示されます。
2. 解像度と垂直走査周波数に、LX でサポートされている値が使用されていることを確認します。詳細は、「**サポートされている画面解像度**」を参照してください。

   注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

Linux の設定の永続化

注: この手順は、使用している Linux® のバージョンによって少し異なる場合があります。

▶ **Linux で設定を永続化するには、以下の手順に従います (プロンプト)。**

1. [System] (システム) メニュー、[Preferences] (設定)、[Personal] (個人)、[Sessions] (セッション) の順に選択します。
2. [Session Options] (セッション オプション) タブをクリックします。

3. [Prompt on log off] (ログオフ時にプロンプト) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。
4. ログアウトするときに、ダイアログで [Save current setup] (現在の設定を保存) オプションを選択します。
5. [OK] (OK) をクリックします。

ヒント: ログアウト時にプロンプトが表示されないようにするには、代わりに以下の手順に従います。

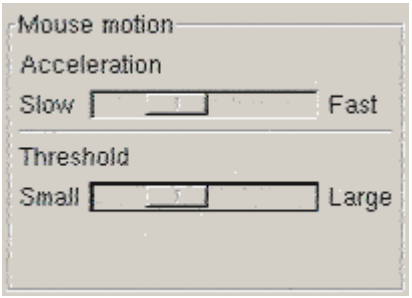
Linux で設定を永続化するには、以下の手順に従います (プロンプトなし)。

1. [Desktop] (デスクトップ)、[Control Center] (コントロールセンタ)、[System] (システム)、[Sessions] (セッション) の順にを選択します。
2. [Session Options] (セッション オプション) タブをクリックします。
3. [Prompt on the log off] (ログオフ時にプロンプト) チェックボックスをオフにします。
4. [Automatically save changes to the session] (セッションに対する変更を自動保存) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションが自動的に保存されます。

Sun Solaris の設定

Sun™ Solaris™ を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定します。そのためには、以下の操作を行います。
   - グラフィカル ユーザ インタフェースを使用する場合



   - コマンド ラインを使用する場合 *xset mouse a t ″a″* は加速 (acceleration)、*″t″* はしきい値 (threshold) を意味します。
2. すべての KVM ターゲット サーバは、LX でサポートされているいずれかの表示解像度に設定する必要があります。Sun マシンで一般的にサポートされる解像度を以下に示します。

表示解像度	垂直操作周波数	縦横比
1600 x 1200	60 Hz	4:3
1280 x 1024	60、75、85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60、70、75、85 Hz	4:3
800 x 600	56、60、72、75、85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60、72、75、85 Hz	4:3

3. Solaris オペレーティング システムを実行している KVM ターゲット サーバのビデオ出力は、VGA である必要があります（コンポジット Sync ではなく H-and-V sync）。

Sun のビデオ カード出力をコンポジット Sync からデフォルト以外の VGA 出力に変更するには、以下の手順に従います。

1. Stop+A コマンドを発行して、bootprom モードに移行します。
2. 以下のコマンドを発行して、出力解像度を変更します。*setenv output-device screen:r1024x768x70*
3. 次に、`boot` コマンドを実行して、サーバを再起動します。

別の方法として、ラリタンの代理店からビデオ出力アダプタを購入することもできます。

環境	対応するビデオ出力アダプタ
Sun 13W3、コンポジット Sync 出力	APSSUN II Guardian コンバータ
Sun HD15、コンポジット Sync 出力	HD15 から 13W3 への変換用の 1396C コンバータ、およびコンポジット Sync をサポートするための APSSUN II Guardian コンバータ
Sun HD15、独立同期出力	APKMSUN Guardian コンバータ

注: 一部の Sun サーバでは、縁が暗い標準の Sun の背景画面が正確に中央に配置されないことがあります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

マウスの設定

マウスを設定するには、以下の手順に従います (Sun Solaris 10.1)。

1. ランチャーを選択します。アプリケーション マネージャ - デスクトップ コントロールが表示されます。
2. マウス スタイル マネージャを選択します。[Style Manager - Mouse] (スタイル マネージャ - マウス) ダイアログ ボックスが表示されます。
3. 速度のスライダを 1.0 に設定します。
4. しきい値のスライダを 1.0 に設定します。
5. [OK] (OK) をクリックします。

コマンド ラインに対するアクセス

1. 右クリックします。
2. [Tool] (ツール)、[Terminal] (ターミナル) の順に選択します。ターミナル ウィンドウが表示されます (ルートでコマンドを発行することをお勧めします)。

ビデオ設定 (POST)

Sun システムには、2 種類の解像度設定があります。POST の解像度と GUI の解像度です。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

現在の POST の解像度を確認するには、以下の手順に従います。

- 次のコマンドを root として実行します。`# eeprom output-device`

POST の解像度を変更するには、以下の手順に従います。

1. `# eeprom output-device=screen:r1024x768x75` を実行します。
2. ログアウトするか、コンピュータを再起動します。

ビデオ設定 (GUI)

GUI の解像度は、お使いのビデオ カードに応じたコマンドを使用して確認および設定できます。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

カード	解像度の確認	解像度の変更
32 ビット	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
64 ビット	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
32 ビットおよび 64 ビット	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。

IBM AIX 5.3 の設定

IBM® AIX™ 5.3 を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

▶ マウスを設定するには、以下の手順に従います。

1. ランチャーに移動します。
2. [Style Manager] (スタイル マネージャ) を選択します。
3. [Mouse] (マウス) をクリックします。[Style Manager – Mouse] (スタイル マネージャ – マウス) ダイアログ ボックスが表示されます。
4. スライダを使用して、[Mouse acceleration] (マウスの加速) を 1.0 に設定し、[Threshold] (しきい値) を 1.0 に設定します。
5. [OK] (OK) をクリックします。

▶ ビデオを設定するには、以下の手順に従います。

1. ランチャーから、[Application Manager] (アプリケーション マネージャ) を選択します。

2. [System_Admin] を選択します。
3. [Smit]、[Devices] (デバイス)、[Graphic Displays] (グラフィック表示)、[Select the Display Resolution and Refresh Rate] (表示解像度と垂直操作周波数の選択) の順に選択します。
4. お使いのビデオ カードを選択します。
5. [List] (リスト) をクリックします。表示モードの一覧が表示されます。
6. LX でサポートされている解像度および垂直走査周波数を選択します。詳細は、「サポートされている画面解像度」を参照してください。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

UNIX の設定の永続化

注: これらの手順は、お使いの UNIX® の種類 (例: Solaris™、IBM® AIX™) および特定のバージョンによって少し異なる可能性があります。

---

1. **[Style Manager] (スタイル マネージャ)、[Startup] (起動) の順に選択します。[Style Manager – Startup] (スタイル マネージャ – 起動) ダイアログ ボックスが表示されます。**
2. [Logout Confirmation] (ログアウトの確認) ダイアログ ボックスで、[On] (オン) オプションを選択します。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。

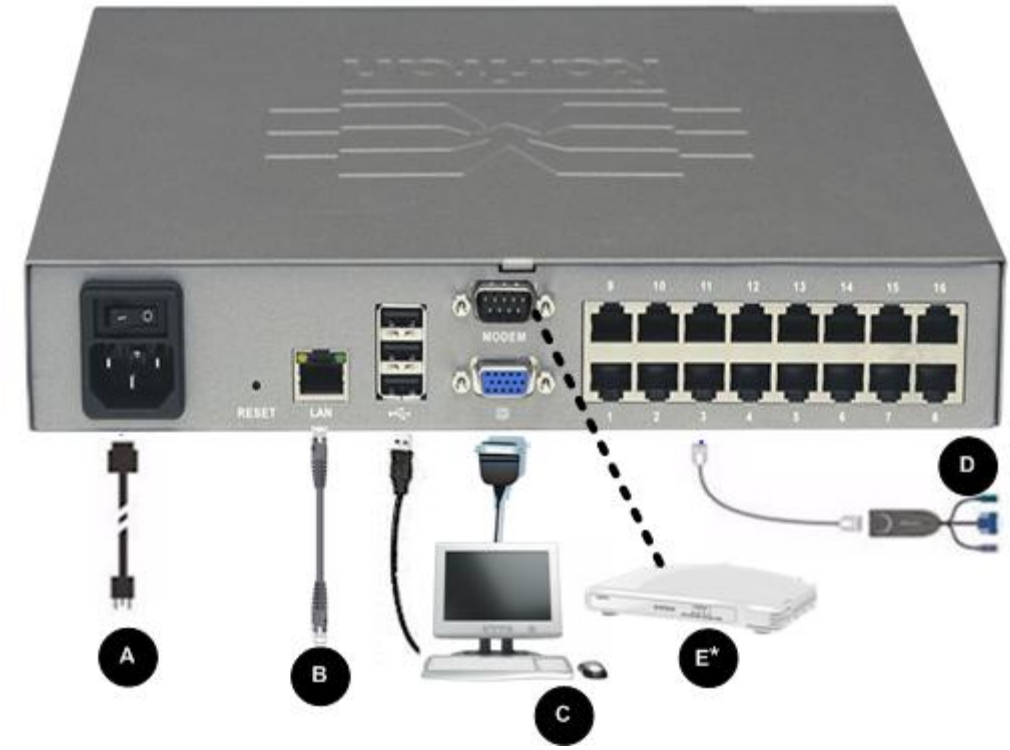
Apple Macintosh の設定

Apple Macintosh® オペレーティング システムを実行している KVM ターゲット サーバに対しては、D2CIM-VUSB およびずれないマウス機能を使用する方法が推奨されます。

手順 2: ネットワーク ファイアウォールの設定

LX へのリモート アクセスを有効にするには、ネットワークおよびファイアウォールにおいて、TCP ポート 5000 での通信が許可されている必要があります。あるいは、別の TCP ポートを使用するように LX を設定し、その TCP ポートでの通信を許可します。Web ブラウザで LX にアクセスできるようにするには、ファイアウォールで TCP ポート 443 (標準 HTTPS) へのアクセスを許可する必要があります。TCP ポート 80 (標準 HTTP) にアクセスすると、HTTP 要求が自動的に HTTPS にリダイレクトされます。

手順 3: 装置の接続



A. AC 電源

▶ **電源を接続するには、以下の手順に従います。**

- 付属の AC 電源コードを LX と AC 電源コンセントに接続します。

B. ネットワーク ポート

▶ **ネットワークを接続するには、以下の手順に従います。**

- 標準 Ethernet ケーブル（付属品）をネットワーク ポートから Ethernet スイッチ、ハブ、またはルータに接続します。

C. ローカル アクセス ポート (ローカル PC)

LX のローカル アクセス ポートを使用することによって、ラックからターゲット サーバに簡単にアクセスできます。ローカル アクセス ポートはインストールおよび設定に必要ですが、それ以降の使用についてはオプションです。ローカル アクセス ポートでは、管理およびターゲット サーバへのアクセスに LX ローカル コンソールのグラフィカル ユーザ インタフェースも使用できます。 詳細については、「LX のローカル ポートの設定」を参照してください。

▶ **ローカル ポートに接続するには、以下の手順に従います。**

- マルチシンク VGA モニタ、マウス、キーボードを各ローカル ユーザ ポートに接続します。キーボードとマウスは、USB 接続のものを使用します。接続ポートは、LX の背面パネルにあります。

接続	説明
モニタ	標準マルチシンク VGA モニタを HD15 (メス) ビデオ ポートに接続します。
キーボード	標準 USB キーボードを USB タイプ A (メス) ポートのいずれかに接続します。
マウス	標準 USB マウスを USB タイプ A (メス) ポートのいずれかに接続します。

D. ターゲット サーバ ポート

LX のローカル アクセス ポートを使用することによって、ラックからターゲット サーバに簡単にアクセスできます。ローカル アクセス ポートはインストールおよび設定に必要ですが、それ以降の使用についてはオプションです。ローカル アクセス ポートでは、管理およびターゲット サーバへのアクセスに LX ローカル コンソールのグラフィカル ユーザ インタフェースも使用できます。 詳細については、「LX のローカル ポートの設定」を参照してください。

▶ **ターゲット サーバを LX に接続するには、以下の手順に従います。**

1. 適切なコンピュータ インタフェース モジュール (CIM) を使用します。 互換性のある CIM については、「*サポートされているオペレーティング システム (クライアント)*『*206*p. 』」を参照してください。

2. CIM の UTP (Cat5/5e/6) ケーブルをターゲット サーバのビデオ ポートに接続します。ターゲット サーバのビデオが、サポートされている解像度と垂直走査周波数に設定されていることを確認します。Sun サーバの場合は、ターゲット サーバのビデオ カードがコンポジット Sync ではなく標準 VGA (H-and-V Sync) を出力するように設定されていることを確認してください。
3. CIM のキーボード/マウス コネクタを、ターゲット サーバの該当するポートに接続します。標準ストレート UTP (Cat5/5e/6) ケーブルを使って、CIM を LX デバイスの背面の使用可能なサーバ ポートに接続します。

注: DCIM-USB G2 の背面には小さいスライド型スイッチがあります。PC ベースの USB ターゲット サーバの場合はスイッチを P にします。Sun の USB ターゲット サーバの場合はスイッチを S にします。

変更後のスイッチ位置が有効になるのは、CIM に給電し直した後です。CIM に給電し直すには、ターゲット サーバから USB コネクタをいったん取り外し、数秒経ってから再度取り付けます。

E. モデム ポート (オプション)

LX は、LAN/WAN が利用できない場合でもリモート アクセス用の専用モデムポートを搭載しています。ストレート シリアル (RS-232) ケーブルを使用して、外付けシリアル モデムを LX の背面にある「MODEM」のラベルの付いたポートに接続します。認定済みモデムのリストについては、「***仕様*** 『*204*p. 』」を、モデムの設定については「***モデムを設定する*** 『*141*p. の*"モデムの設定"*参照 』」を参照してください。

注: モデムは、CD (キャリア検出) 設定を有効にするように設定することをお勧めします。

手順 4: LX の設定

LX デバイスの電源を初めてオンにしたときは、LX ローカル コンソールで以下の操作を行う必要があります。

- デフォルト パスワードの変更
- IP アドレスの割り当て
- KVM ターゲット サーバの命名

Web ブラウザを使用して LX をリモートで設定できます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。

デフォルト パスワードの変更

LX の出荷時には、デフォルトのパスワードが設定されています。LX を初めて起動したときは、このパスワードを変更する必要があります。

▶ **デフォルトのパスワードを変更するには、以下の手順に従います。**

1. 本体が起動したら、デフォルトのユーザ名（admin）とパスワード（raritan）を入力します。[ログイン] をクリックします。
2. 古いパスワード（raritan）を入力し、新しいパスワードを入力した後、もう一度新しいパスワードを入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。[適用] をクリックします。[確認] ページで [OK] をクリックします。

注: デフォルトのパスワードは Raritan Multi-Platform Client (MPC) からも変更できます。

IP アドレスの割り当て

ここでは、[ネットワーク設定] ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作の詳細については、「*ネットワーク設定* 『*128*p. 』」を参照してください。

▶ **IP アドレスを割り当てるには、以下の手順に従います。**

1. [Device Settings]（デバイス設定）の [Network]（ネットワーク）を選択します。[ネットワーク設定]（Network Settings）ページが開きます。
2. LX デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4]（IPv4）セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration]（IP 自動設定）ドロップダウンから [None]（なし）を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration]（IP 自動設定）ドロップダウンから [DHCP]（DHCP）を選択した場合は、優先ホスト名を入力します。
   e. [IP Auto Configuration]（IP 自動設定）を選択します。次のオプションを使用できます。
   - [None]（なし）（静的 IP）– このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

LX はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。

- [DHCP] (DHCP) – DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ（クライアント）によって Dynamic Host Configuration Protocol が使用されます。

  このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名）を入力します（DHCP のみ)。最大 63 文字まで使用できます。

4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。
   a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。
   b. [Global/Unique IP Address] (グローバル/一意の IP アドレス）を入力します。これは、LX に割り当てられる IP アドレスです。
   c. [Prefix Length] (固定長）を入力します。これは、IPv6 アドレスで使用されるビット数です。
   d. [Gateway IP Address] (ゲートウェイ IP アドレス）を入力します。
   e. [Link-Local IP Address] (リンク – ローカル IP アドレス)。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索で、またはルータが存在しない場合に使用されます。
   [Read-Only] (読み取り専用)
   f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。**[Read-Only] (読み取り専用)**
   g. [IP Auto Configuration] (IP 自動設定）を選択します。次のオプションを使用できます。

   - [None] (設定しない) – 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します（静的 IP)。推奨されるデフォルトのオプションです。

     [IP auto configuration] (IP 自動設定）で [None] (設定しない）を選択すると、[Network Basic Settings] (ネットワーク基本設定）フィールド ([Global/Unique IP Address] (グローバル/一意の IP アドレス)、[Prefix Length] (固定長)、[Gateway IP Address] (ゲートウェイ IP アドレス)) が有効になり、IP アドレスを手動で設定できるようになります。

   - [Router Discovery] (ルータ検出) – このオプションを使用して、直接接続されるサブネットにのみ適用される [Link Local] (リンクローカル）を超える [Global] (グローバル）または [Unique Local] (一意ローカル）を意味する IPv6 アドレスを自動的に割り当てます。

5. DHCPが選択されており、[Obtain DNS Server Address](DNS サーバ アドレスを取得する)が有効になっている場合は、[Obtain DNS Server Address Automatically](DNS サーバ アドレスを自動的に取得する)を選択します。[Obtain DNS Server Address Automatically](DNS サーバ アドレスを自動的に取得する)を選択した場合は、DHCP サーバから得られた DNS 情報が使用されます。
6. [Use the Following DNS Server Addresses](次の DNS サーバ アドレスを使用する)が選択されている場合は、DHCPが選択されているかどうかにかかわらず、このセクションに入力したアドレスを使用して DNS サーバに接続されます。

   [Use the Following DNS Server Addresses](次の DNS サーバ アドレスを使用する)が選択されている場合は、以下の情報を入力します。これらのアドレスは、停電のためにプライマリ DNS サーバ接続が失われた場合に使用されるプライマリおよびセカンダリの DNS アドレスです。

   a. プライマリ DNS サーバ IP アドレス
   b. セカンダリ DNS サーバ IP アドレス
7. 完了したら[OK]をクリックします。

[ネットワーク設定]ページのこのセクションの設定については、「LAN インタフェース設定」を参照してください。

---

*注: 一部の環境では、[LAN Interface Speed & Duplex](LAN インタフェースの速度と二重化)のデフォルトである[Autodetect](自動検出)(自動ネゴシエーション)が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、LX の[LAN Interface Speed & Duplex](LAN インタフェースの速度と二重化)フィールドを[100 Mbps/Full Duplex](またはネットワークに合ったオプション)に設定することで問題を解決できます。詳細については、「***ネットワーク設定 『128p. 』***」を参照してください。*

日付/時刻の設定 (オプション)

▶ **日付と時刻を設定するには、以下の手順に従います。**

1. [デバイス設定]の[日付/時刻]を選択します。[日付/時刻の設定]ページが開きます。
2. [タイム ゾーン]ドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、[夏時間用の調整]チェックボックスをオンにします。
4. 日付と時刻の設定で用いる方法を選択します。

- [ユーザによる時刻定義]: 日付と時刻を手動で入力するには、このオプションを選択します。[ユーザによる時刻定義] オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
- [NTP サーバと同期]: 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期するには、このオプションを選択します。

5. [NTP サーバと同期] オプションを選択した場合は、以下の手順に従います。
   a. プライマリ タイム サーバの IP アドレスを入力します。
   b. セカンダリ タイム サーバの IP アドレスを入力します。**(オプション)**
6. [OK] をクリックします。

ターゲット サーバの命名

▶ **ターゲット サーバに名前を付けるには、以下の手順に従います。**

1. まだすべてのターゲット サーバを接続していない場合は、接続します。装置の接続方法の詳細については、「**手順 3: 装置の接続**」を参照してください。
2. LX ローカル コンソールを使用して、[デバイス設定] の [ポート設定] を選択し、名前を付けるターゲット サーバの [ポート名] をクリックします。
3. サーバの名前を入力します。名前には最大 32 文字の英数字と特殊文字を使用できます。[OK] をクリックします。

ターゲット名で使用できる有効な特殊文字

ﾎﾄﾗﾖ	説明	ﾎﾄﾗﾖ	説明
!	感嘆符	;	セミコロン
″	二重引用符	=	等号
#	シャープ記号	>	大なり記号
$	ドル記号	?	疑問符
%	パーセント記号	@	アット記号
&	アンパサンド	[	左角かっこ
(	左かっこ	¥	バックスラッシュ
)	右かっこ	]	右角かっこ
*	アスタリスク	^	キャレット

ホトラヨ	説明	ホトラヨ	説明
+	プラス記号	_	アンダースコア
,	コンマ	`	低アクセント
-	ダッシュ	{	左中かっこ
.	ピリオド	|	パイプ記号
/	前方スラッシュ	}	右中かっこ
<	小なり記号	~	ティルデ
:	コロン		

リモート認証

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、LX には認証要求を外部認証サーバへ転送する機能があります。LDAP/LDAPS と RADIUS の 2 つの外部認証プロトコルがサポートされています。

Microsoft Active Directory についての注意事項

Microsoft® Active Directory® は、LDAP/LDAPS プロトコルをネイティブに使用し、LDAP/LDAPS サーバおよび LX の認証元として機能することが可能です。IAS (インタフェース認可サーバ) のコンポーネントを装備している場合、Microsoft Active Directory サーバは、RADIUS 認証元としても機能します。

ユーザ グループおよびユーザを作成する

LX にアクセスするためには、初期設定の一環としてユーザ グループおよびユーザを定義する必要があります。

LX では、システムによって定義されているデフォルトのユーザ グループを使用して、グループの作成および目的に合った適切な許可の指定を行えるようになります。

LX にアクセスするには、ユーザ名とパスワードが必要です。この情報は、LX にアクセスしようとしているユーザを認証するために使用されます。ユーザ グループやユーザの追加方法および編集方法の詳細については、**「ユーザ管理 『104p. の"[User Management] (ユーザ管理)"参照 』」を参照してください。**

手順 5: LX リモート コンソールの起動

▶ **LX リモート コンソールを起動するには、以下の手順に従います。**

1. LX にネットワークを介して接続でき、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、任意のコンピュータからログインします (JRE® は *Java の Web サイト http://java.sun.com/*から入手できます)。
2. サポートされている Web ブラウザ (Internet Explorer® や Firefox® など) を起動します。
3. URL として、「*http://IP-ADDRESS*」または .NET の場合には「*http://IP-ADDRESS/akc*」と入力します。IP-ADDRESS は、LX に割り当てられた IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた LX の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (LX では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
4. ユーザ名とパスワードを入力します。[ログイン] をクリックします。

リモートからのターゲット サーバのアクセスと制御

LX の [ポート アクセス] ページには、すべての LX ポート、接続中のターゲット サーバ、ターゲット サーバの状態およびその可用性が表示されます。

ターゲット サーバへのアクセス

▶ **ターゲット サーバにアクセスするには、以下の手順に従います。**

1. アクセスしたいターゲット サーバのポート名をクリックします。[ポート アクション] メニューが開きます。
2. [ポート アクション] メニューの [接続] をクリックします。[KVM] ウィンドウが開き、ターゲットへの接続が示されます。

ターゲット サーバの切り替え

▶ **KVM ターゲット サーバを切り替えるには、以下の手順に従います。**

1. ターゲット サーバを使用しているときに、LX の [ポート アクセス] ページを開きます。
2. アクセスするターゲットの [ポート名] をクリックします。[ポート アクション] メニューが表示されます。
3. [ポート アクション] メニューの [切り替え元] を選択します。選択した新しいターゲット サーバが表示されます。

ターゲット サーバの切断

▶ **ターゲット サーバを切断するには、以下の手順に従います。**

- 切断するターゲットのポート名をクリックします。[ポート アクション] メニューが表示されたら、[切断] をクリックします。

手順 6: キーボード言語の設定 (オプション)

注: 英語 (アメリカ)/インターナショナル キーボードを使用している場合は、この手順を実行する必要はありません。

英語 (アメリカ) 以外の言語を使用する場合、キーボードを適切な言語に設定する必要があります。また、クライアント マシンおよび KVM ターゲット サーバのキーボード言語を同じにする必要があります。

キーボード レイアウトを変更する方法の詳細については、お使いのオペレーティング システムのマニュアルを参照してください。

キーボード レイアウト コードの変更 (Sun ターゲット)

この手順は、DCIM-SUSB を使用していて、キーボード レイアウトを別の言語に変更する場合に使用します。

▶ **キーボード レイアウト コードを変更するには、以下の手順に従います (DCIM-SUSB のみ)。**

1. Sun™ ワークステーション上で [テキスト エディタ] ウィンドウを開きます。
2. Num Lock キーが有効であることを確認した後、キーボードの左の Ctrl キーと Del キーを押します。Caps Lock ライトが点滅して、CIM がレイアウト コード変更モードであることを示します。テキスト ウィンドウに、「`Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`」と表示されます。
3. 適切なレイアウト コード (たとえば日本語キーボードは *31*) を入力します。
4. Enter キーを押します。
5. デバイスの電源を切った後、再度電源を入れます。DCIM-SUSB がリセット (電源の再投入) されます。
6. 入力した文字が正しく表示されることを確認します。

手順 7: カスケード接続の設定 (オプション)

LX および汎用カスケード接続は、LX でサポートされています。この機能の詳細については、「**デバイス管理** 『128p. 』」セクションを参照してください。

ベース LX デバイスのターゲット サーバ ポートとカスケード接続 LX デバイスのローカル アクセス ポート（ビデオ/キーボード/マウス ポート）を、D2CIM-DVUSB で接続します。

▶ ティアー接続を有効にするには

1. ティアー接続構成内のベース デバイスで、[Device Settings]（デバイス設定）の [Device Services]（デバイス サービス）を選択します。[Device Services Settings]（デバイス サービス設定）ページが表示されます。
2. [Enable Tiering as Base]（ベースとしてのティアー接続を有効にする）を選択します。
3. [Base Secret]（ベース秘密ワード）フィールドに、ベース デバイスとティアー接続デバイスの間で共有される秘密ワードを入力します。この秘密ワードは、ティアー接続デバイスでベース デバイスを認証する際に必要となります。同じ秘密ワードをティアー接続デバイスに対して入力します。
4. [OK]（OK）をクリックします。
5. ティアー接続デバイスを有効にします。ティアー接続デバイスで、[Device Settings]（デバイス設定）の [Local Port Settings]（ローカル ポート設定）を選択します。
6. このページの [Enable Local Ports]（ローカル ポートを有効にする）セクションで、[Enable Local Port Device Tiering]（ローカル ポート デバイスのティアー接続を有効にする）を選択します。
7. [Tier Secret]（ティアー接続秘密ワード）フィールドに、ベース デバイスの [Device Settings]（デバイス設定）ページで入力したのと同じ秘密ワードを入力します。
8. [OK]（OK）をクリックします。

Ch 3 ターゲット サーバの使用

この章の内容

LX インタフェース

LX には、いつでも、どこからでもターゲットへの簡単なアクセスを可能にするいくつかのユーザ インタフェースが用意されています。このようなユーザ インタフェースには、LX ローカル コンソール、LX リモート コンソール、Virtual KVM Client (VKC)、Active KVM Client (AKC)、および Multi-Platform Client (MPC) があります。以下の表に、ターゲット サーバのアクセスおよび管理のためにこれらのインタフェースをローカルおよびリモートで使用できるかどうかを示します。

ユーザ インタフェース	ローカル		リモート	
	アクセス	管理	アクセス	管理
LX ローカル コンソール	✓	✓		
LX リモート コンソール			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

ヘルプの以降のセクションでは、以下のインタフェースを使用した LX へのアクセスおよびターゲット管理の方法について説明します。

- ローカル コンソール
- リモート コンソール
- Virtual KVM Client
- Multi-Platform Client

LX ローカル コンソール インタフェース: LX デバイス

サーバ ラックに設置した LX の場合は、LX ローカル コンソールを介して、標準 KVM 管理を行います。LX ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。

LX ローカル コンソールと LX リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

[LX Local Console Factory Reset] (LX ローカル コンソール ファクトリ リセット) オプションは、LX ローカル コンソールには用意されていますが、LX リモート コンソールには用意されていません。

LX リモート コンソール インタフェース

LX リモート コンソールは、ブラウザ ベースのグラフィカル ユーザ インタフェースで、このコンソールを通じて、LX に接続されている KVM ターゲット サーバおよびシリアル ターゲットにログインして、LX をリモート管理できます。

LX リモート コンソールは、接続されているターゲット サーバへのデジタル接続を提供します。LX リモート コンソールを使用して KVM ターゲット サーバにログインすると、Virtual KVM Client のウィンドウが開きます。

LX ローカル コンソールと LX リモート コンソールのグラフィカル ユーザ インタフェースには多くの類似点があります。相違点については、ユーザ マニュアルに記載されています。以下のオプションは LX リモート コンソールに用意されていますが、LX ローカル コンソールには用意されていません。

- 仮想メディア
- [Favorites] (お気に入り)
- [Backup/Restore] (バックアップ/リストア)
- [Firmware Upgrade] (ファームウェアのアップグレード)
- SSL 証明書

LX リモート コンソールの起動

重要: ブラウザの種類を問わず、LX リモート コンソールを起動するためには、デバイスの IP アドレスからのポップアップを許可する必要があります。

お使いのブラウザおよびセキュリティの設定により、セキュリティと証明書に関する各種の警告が表示されることがあります。LX リモート コンソールを起動するには、これらの警告を承諾する必要があります。

セキュリティと証明書に関する警告メッセージに対して以下のオプションをオンにすることにより、それ以降にログインしたときに表示される警告メッセージを減らすことができます。

- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]

LX リモート コンソールを起動するには、以下の手順に従います。

1. LX にネットワークを介して接続でき、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、任意のコンピュータからログインします (JRE® は *Java の Web サイト http://java.sun.com/*から入手できます)。
2. サポートされている Web ブラウザ (Internet Explorer® や Firefox® など) を起動します。
3. URL として、「*http://IP-ADDRESS*」または .NET の場合には「*http://IP-ADDRESS/akc*」と入力します。IP-ADDRESS は、LX に割り当てられた IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた LX の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (LX では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
4. ユーザ名とパスワードを入力します。初めてログインする場合は、工場出荷時のデフォルト ユーザ名 (admin) とパスワード (すべて小文字の raritan) を使用してログインします。デフォルトのパスワードを変更するように求められます。[ログイン] をクリックします。

リモート コンソールを介して利用できる LX の機能の詳細については、「*Virtual KVM Client および Active KVM Client (AKC)* 『*56*p. の*"Virtual KVM Client (VKC) および Active KVM Client (AKC)"*参照 』」を参照してください。

インタフェースおよび画面操作

LX インタフェース

LX リモート コンソール インタフェースと LX ローカル コンソール インタフェースは、デバイス設定および管理、ターゲット サーバのリストおよび選択用に、Web ベース インタフェースを備えています。オプションは複数のタブに配置されています。

正常にログインすると、[ポート アクセス] ページが表示され、すべてのポートについて、そのステータスと可用性が表示されます。2 つのタブ [ポート別表示] および [スキャン設定] がページ上に表示されます。[ポート別表示] タブの列の見出しをクリックして、ポート番号、ポート名、ステータス ([アップ] および [ダウン])、可用性 ([アイドル]、[接続済み]、[ビジー]、[使用不可能]、[接続中]) で並べ替えを行います。ページに表示されるポート数を変更するには、ページの右下にある [1 ページ当たりの行] フィールドに数値を入力し、[設定] をクリックします。 詳細については、「*[ポート アクセス] ページ* 『*45*p. 』」を参照してください。

[スキャン設定] タブを使用して、LX に接続されているターゲットを 32 台までスキャンできます。「*ポートのスキャン* 『*48*p. 』」を参照してください。

左パネル

LX インタフェースの左パネルにある情報は次のとおりです。なお、一部の情報は特定の条件下でのみ表示されます。たとえば、自分が特定のユーザである場合や、特定の機能を利用している場合などです。各情報が表示される条件もこの表に示します。

情報	説明	表示される条件
[日時およびセッション]	現在のセッションが開始した日時。	常時
ユーザ	ユーザ名。	常時
[状態]	アプリケーションの現在の状態（アイドルまたはアクティブ）。アイドル状態の場合、セッションがアイドル状態になっている時間が追跡および表示されます。	常時
[あなたの IP アドレス]	LX にアクセスする際に使用された IP アドレス。	常時
[最終ログイン日時]	最後にログインした日時。	常時
[デバイス情報]	使用している LX に特有の情報。	常時
[デバイス名]	デバイスに割り当てられている名前。	常時
[IP アドレス]	LX の IP アドレス。	常時
[ファームウェア]	ファームウェアの現在のバージョン。	常時
[デバイス モデル]	LX のモデル。	常時
[ベース デバイスとして設定] または [カスケード接続デバイスとして設定]*	カスケード接続を使用している場合、現在アクセスしている LX がベースデバイスとカスケード接続デバイスのどちらであるかが表示されます。	LX がカスケード接続構成の一要素になっている場合

情報	説明	表示される条件
[ポートの状態]	LX によって現在使用されているポートのステータス。	常時
[接続中のユーザー]	現在 LX に接続している、ユーザ名と IP アドレスによって識別されるユーザ。	常時
[オンライン ヘルプ]	オンライン ヘルプへのリンク。	常時
[お気に入りデバイス]	「*お気に入りの管理* 『*51*p. 』」を参照してください。	常時

LX コンソールでの案内

LX コンソール インタフェースでは、いくつかの方法でナビゲーションや選択を行うことができます。

▶ **オプションを選択するには、以下のいずれかの手順に従います。**

- タブをクリックします。利用可能なオプションのページが表示されます。
- タブ上にカーソルを移動し、メニューから適切なオプションを選択します。
- 表示されるメニュー階層（階層リンク）からオプションを直接クリックします。

▶ **画面に収まらないページをスクロールするには、以下のいずれかの手順に従います。**

- キーボードの Page Up キーと Page Down キーを使用します。
- 右側にあるスクロール バーを使用します。

[ポート アクセス] ページ

LX リモート コンソールへのログオンが正常に完了すると、[ポート アクセス] ページが表示されます。デフォルトで、[ポート アクセス] ページには [ポート別表示] タブが表示されます。このページには、LX のポート、各ポートに接続されている KVM ターゲット サーバ、および各ターゲット サーバのステータスと稼動状態が一覧表示されます。[ポート アクセス] ページは、LX に接続されている KVM ターゲット サーバへのアクセスを提供します。KVM ターゲット サーバは、LX デバイスを介して制御するサーバです。これらは、デバイスの背面にある LX ポートに接続されます。

注: KVM ターゲット サーバへの接続ごとに、新しい Virtual KVM Client ウィンドウが開きます。

ティアー接続構成にしており、ベース LX デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、 カスケード接続デバイスは、[ポート アクセス] ページでカスケード接続デバイス名の左にある展開矢印アイコン ▶ をクリックすると表示されます。カスケード接続の詳細については、「***カスケード接続の設定および有効化*** *『135*p. *』*」を参照してください。

ポート スキャン機能には、[ポート アクセス] ページの [スキャンの設定] タブからアクセスします。この機能によって、スキャンするターゲットのセットを定義できます。スキャンしたターゲットのサムネイル表示も使用できます。サムネイルを選択すると、そのターゲットが Virtual KVM Client ウィンドウに表示されます。

▶ [Port Access] (ポート アクセス) ページを使用するには

1. LX リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。

   KVM ターゲット サーバは当初ポート番号順に並んでいますが、列のいずれかを基準に表示順を変更できます。

   - [Port Number] (ポート番号) - 1 から LX デバイスで使用できるポートの合計数までの番号が振られています。
   - [ポート名]: LX ポートの名前です。最初は、「Dominion-LX-Port#」に設定されていますが、わかりやすい名前に変更できます。[ポート名] のリンクをクリックすると、[ポート アクション] メニューが表示されます。

     注: ポート (CIM) 名にアポストロフィ (' ") を使用することはできません。

   - [タイプ]: サーバまたは CIM のタイプです。
   - [ステータス]: 標準サーバのステータスは [アップ] または [ダウン] のどちらかです。
   - [可用性]: サーバの可用性です。

2. アクセスするターゲット サーバのポート名をクリックします。[ポート アクション] メニューが表示されます。使用可能なメニュー オプションの詳細については、「[ポート アクション] メニュー」を参照してください。
3. [ポート アクション] メニューから、目的のメニュー コマンドを選択します。
4. スキャンするポートのセットは、LX でスキャン設定機能を使用して定義します。「*ポートのスキャン 『48p. 』*」を参照してください。

表示順を変更したり同じページにさらにポートを表示したりするには、以下の手順に従います。

1. 並べ替えで基準にする列の見出しをクリックします。その列に基づいて KVM ターゲット サーバのリストが並べ替えられます。
2. [1 ページ当たりの行] に、ページに表示するポート数を入力し、[設定] をクリックします。

[ポート アクション] メニュー

[ポート アクセス] リストで [ポート名] をクリックすると、[ポート アクション] メニューが表示されます。対象のポートに対して適切なメニュー オプションを選択して実行します。[ポート アクション] メニューには、ポートのステータスと可用性に応じて、その時点で利用可能なオプションだけが表示されます。

- [Connect] (接続) – ターゲット サーバへの新しい接続を作成します。LX リモート コンソールの場合は、新しい Virtual KVM Client ページが表示されます。LX ローカル コンソールの場合は、ローカル ユーザ インタフェースからターゲット サーバに表示が切り替わります。ローカル ポートで切り替えを行うためには、LX ローカル コンソール インタフェースが表示されている必要があります。ローカル ポートからのホット キー切り替えも利用できるようになりました。

  注:すべての接続がビジー状態の場合、LX リモート コンソールで使用可能なポートに対してこのオプションは使用できません。

- [Switch From] (切り替え元) – 既存の接続から選択したポート (KVM ターゲット サーバ) に切り替えます。このメニュー項目は、KVM ターゲットに対してのみ使用できます。このオプションは Virtual KVM Client が開いている場合にのみ表示されます。

  注: LX ローカル コンソールでは、このメニュー項目は使用できません。

- [Disconnect](切断) – このポートを切断し、このターゲット サーバの Virtual KVM Client ページを閉じます。このメニュー項目は、ポート ステータスが [Up](アップ) かつ [Connected](接続済み) の場合、または [Up](アップ) かつ [Busy](ビジー) の場合にのみ使用できます。

注: LX ローカル コンソールでは、このメニュー項目は使用できません。ローカル コンソールで切り替えたターゲットを切断する唯一の方法は、ホットキーを使用することです。

ポートのスキャン

LX には、選択したターゲットを検索してそれをスライド ショー ビューで表示するポート スキャン機能が用意されています。これを使用すると、最大 32 のターゲットを一度にモニタできます。ターゲットに接続することも、必要に応じて特定のターゲットをフォーカスすることもできます。スキャン対象は、標準ターゲット、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。

注: カスケード接続デバイスのスキャンは、Multi-Platform Client (MPC) ではサポートされていません。

スキャンを開始すると、[Port Scan] (ポート スキャン) ウィンドウが開きます。ターゲットが見つかるたびに、スライド ショーのサムネイルとして表示されます。スライド ショーでは、デフォルト間隔の 10 秒ごとに、またはユーザが指定した間隔に従ってターゲットのサムネイルがスクロールされます。スキャンによってターゲットがスクロールされるときは、スライド ショーでフォーカスされているターゲットがページの中央に表示されます。「***スキャン設定*** *『85*p. *』*」を参照してください。

スライド ショーでサムネイルのローテーションにかかる時間、サムネイルのフォーカス間隔、ページの表示設定は、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Multi-Platform Client (MPC) の [Tools] (ツール) の [Options] (オプション) ダイアログの [Scan Settings] (スキャン設定) タブから変更できます。「***スキャン設定*** *『85*p. *』*」を参照してください。

ターゲット名はサムネイルの下とウィンドウ下部のタスクバーに表示されます。ターゲットがビジーである場合は、ターゲット サーバへのアクセス ページの代わりに空白の画面が表示されます。

各ターゲットのステータスは、ターゲットのサムネイルの下およびタスクバー (ターゲットがローテーションにおいてフォーカスされている場合) に表示される緑、黄色、赤のライトで示されます。ステータス ライトは、以下を示します。

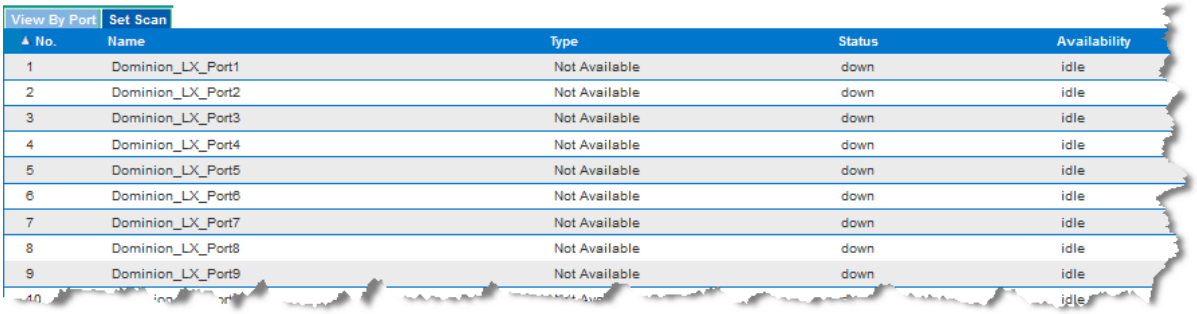
- 緑 – ターゲットはアップ/アイドルまたはアップ/接続済み
- 黄色 – ターゲットはダウンしているが接続済み
- 赤 – ターゲットはダウン/アイドル、ビジー、またはアクセス不可能

この機能は、ローカル ポート、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Multi-Platform Client (MPC) から使用できます。

*注: MPC は、他の Raritan クライアントとは異なる方法を使用してスキャンを開始します。詳細については、『KVM and Serial Client Guide』の「Set Scan Group」を参照してください。リモート コンソールとローカル コンソールでは、スキャンの結果およびオプションが異なります。**「***ポートのスキャン – ローカル コンソール** *『195p. 』」を参照してください。*

ターゲットをスキャンするには、以下の手順に従います。

1. [ポート アクセス] ページの [スキャン設定] タブをクリックします。
2. 各ターゲットの横にあるチェックボックスをオンにしてスキャン対象に含めるターゲットを個別に選択するか、ターゲット列の上部にあるチェックボックスをオンにしてすべてのターゲットを選択します。
3. アップ ステータスのターゲットだけをスキャンに含める場合は、[アップのみ] チェックボックスをオンのままにします。アップかダウンかに関係なくすべてのターゲットを含める場合は、このチェックボックスをオフにします。
4. [スキャン] をクリックしてスキャンを開始します。スキャンされたターゲットは、ページのスライド ショー ビューに表示されます。
5. [オプション] の [一時停止] をクリックすると、スライド ショーが一時停止してターゲット間での移動が停止します。[オプション] の [再開] をクリックするとスライド ショーが再開されます。
6. ターゲットのサムネイルをクリックすると、それが次にスキャンされます。
7. サムネイルをダブルクリックすると、そのターゲットに接続されます。


View By Port | Set Scan

▲ No.	Name	Type	Status	Availability
1	Dominion_LX_Port1	Not Available	down	idle
2	Dominion_LX_Port2	Not Available	down	idle
3	Dominion_LX_Port3	Not Available	down	idle
4	Dominion_LX_Port4	Not Available	down	idle
5	Dominion_LX_Port5	Not Available	down	idle
6	Dominion_LX_Port6	Not Available	down	idle
7	Dominion_LX_Port7	Not Available	down	idle
8	Dominion_LX_Port8	Not Available	down	idle
9	Dominion_LX_Port9	Not Available	down	idle

スキャン オプションの使用

ターゲットのスキャン中は、次のオプションを使用できます。これらのすべてのオプションは、[Expand]（展開）/[Collapse]（折りたたみ）アイコンを除き、[Port Scan]（ポート スキャン）ビューアの左上の [Options]（オプション）メニューから選択します。ウィンドウを閉じると、オプションはデフォルトに戻ります。

サムネイルの表示または非表示

- ウィンドウの左上の [Expand]（展開）/[Collapse]（折りたたみ）アイコン  を使用して、サムネイルを表示または非表示にします。デフォルト表示では展開されています。

サムネイル スライド ショーの一時停止

- [Options]（オプション）の [Pause]（一時停止）を選択すると、あるターゲットから次のターゲットへのサムネイルのローテーションが一時停止します。サムネイルのローテーションはデフォルト設定です。

サムネイル スライド ショーの再開

- [Options]（オプション）の [Resume]（再開）を選択すると、サムネイルのローテーションが再開されます。

[Port Scan] (ポート スキャン) ビューアのサムネイルのサイズ変更

- サムネイルを拡大するには、[Options]（オプション）、[Size]（サイズ）、[360x240] の順に選択します。
- サムネイルを最小化するには、[Options]（オプション）、[Size]（サイズ）、[160x120] の順に選択します。これはデフォルトのサムネイル サイズです。

[Port Scan] (ポート スキャン) ビューアの表示方向の変更

- [Options]（オプション）、[Split Orientation]（分割方向）、[Horizontal]（横）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの下部に沿って表示されます。
- [Options]（オプション）、[Split Orientation]（分割方向）、[Vertical]（縦）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの右側に沿って表示されます。これがデフォルト表示です。

お気に入りの管理

お気に入り機能を利用すると、よく使用するデバイスにすばやくアクセスできます。[ポート アクセス] ページの左下隅（サイドバー）にある [お気に入りデバイス] セクションでは、以下の操作が可能です。

- お気に入りデバイスのリストを作成および管理する。
- よく使用するデバイスにすばやくアクセスする。
- 名前、IP アドレス、または DNS ホスト名別にお気に入りのリストを表示する。
- サブネット上の LX デバイスを検出する（ログインの前および後）。
- 検出された LX デバイスを接続されている Dominion デバイスから取得する（ログインの後）。

お気に入りの LX デバイスにアクセスするには、以下の手順に従います。

- ([Favorite Devices] (お気に入りデバイス) の下に表示されている) デバイス名をクリックします。新しいブラウザが開き、デバイスが表示されます。

お気に入りを名前順に表示するには、以下の手順に従います。

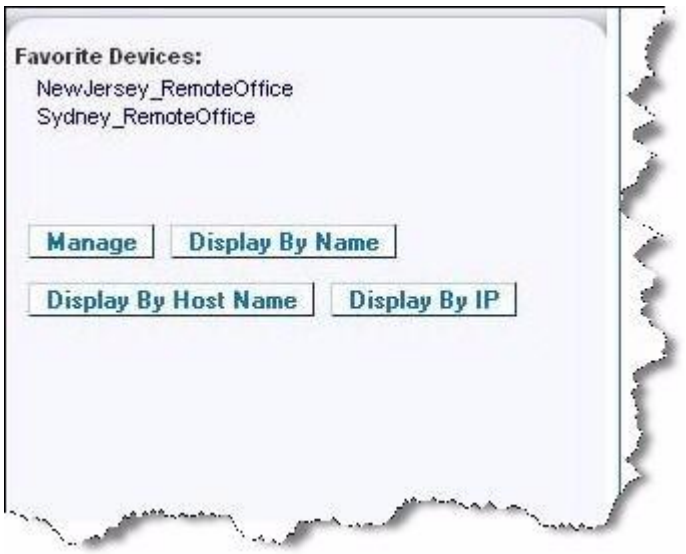
- [Display by Name] (名前順) をクリックします。

お気に入りを IP アドレス順に表示するには、以下の手順に従います。

- [Display by IP] (IP 順) をクリックします。

お気に入りをホスト名順に表示するには、以下の手順に従います。

- [Display by Host Name] (ホスト名順) をクリックします。



[お気に入りの管理] ページ

▶ **[お気に入りの管理] ページを開くには、以下の手順に従います。**

- 左パネルの［管理］をクリックします。次の内容を含む［お気に入りの管理］ページが表示されます。

メニュー	目的
［お気に入りリスト］	お気に入りデバイスのリストを管理します。
［デバイス検出 – ローカル サブネット］	クライアント PC のローカル サブネット上の Raritan デバイスを検出します。
［デバイス検出 – LX サブネット］	LX デバイス サブネット上の Raritan デバイスを検出します。
［お気に入りへの新しいデバイスの追加］	お気に入りリストのデバイスを追加、編集、および削除します。

[お気に入りリスト] ページ

［お気に入りリスト］ページでは、お気に入りリストのデバイスを追加、編集、および削除できます。

▶ **[お気に入りリスト] ページを開くには、以下の手順に従います。**

- ［管理］の［お気に入りリスト］を選択します。［お気に入りリスト］ページが開きます。

ローカル サブネット上のデバイスの検出

ローカル サブネット（LX リモート コンソールが実行されているサブネット）上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ 『52p. 』*」を参照してください。

▶ **ローカル サブネット上のデバイスを検出するには、以下の手順に従います。**

1. ［管理］の［デバイス検出 – ローカル サブネット］を選択します。［デバイス検出 – ローカル サブネット］ページが表示されます。
2. 目的の検出ポートを選択します。

- デフォルトの検出ポートを使用するには、[デフォルト ポート 5000 を使用] チェックボックスをオンにします。
- 別の検出ポートを使用するには、以下の手順に従います。

a. [デフォルト ポート 5000 を使用] チェックボックスをオフにします。
b. [検出ポート] フィールドに、ポート番号を入力します。
c. [保存] をクリックします。

3. [更新] をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. [追加] をクリックします。

▶ 検出されたデバイスにアクセスするには、以下の手順に従います。

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

LX サブネット上のデバイスの検出

デバイス サブネット（LX デバイスの IP アドレスそのもののサブネット）上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ 『52*p. 』」を参照してください。

この機能を使用すると、複数の LX デバイスが相互に作用し合い、自動的にデバイスを検知し構成を拡張します。LX リモート コンソールは、LX のサブネット内の LX デバイスおよびその他の Raritan デバイスを自動的に検出します。

▶ デバイス サブネット上のデバイスを検出するには、以下の手順に従います。

1. [管理] の [デバイス検出 －LX サブネット] を選択します。[デバイス検出 －LX サブネット] ページが表示されます。
2. [更新] をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. [追加] をクリックします。

検出されたデバイスにアクセスするには、以下の手順に従います。

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

お気に入りの追加、削除、および編集

デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。

1. [管理] の [お気に入りへの新しいデバイスの追加] を選択します。[新しいお気に入りの追加] ページが表示されます。
2. わかりやすい説明を入力します。
3. デバイスの IP アドレス/ホスト名を入力します。
4. 必要に応じて検出ポートを変更します。
5. 製品タイプを選択します。
6. [OK] をクリックします。デバイスがお気に入りのリストに追加されます。

お気に入りを編集するには、以下の手順に従います。

1. [お気に入りリスト] ページで、目的の LX デバイスの横にあるチェックボックスをオンにします。
2. [編集] をクリックします。[編集] ページが表示されます。
3. 必要に応じてフィールドを更新します。
   - 説明
   - [IP アドレス/ホスト名]: LX デバイスの IP アドレスを入力します。
   - [ポート] (必要な場合)
   - [製品タイプ]
4. [OK] をクリックします。

お気に入りを削除するには、以下の手順に従います。

重要: お気に入りを削除する場合は注意してください。削除を確認するプロンプトは表示されません。

1. 目的の LX デバイスの横にあるチェックボックスをオンにします。
2. [削除] をクリックします。お気に入りのリストからお気に入りが削除されます。

ログアウト

LX を終了するには、以下の操作を行います。

- ページの右上隅の [Logout] (ログアウト) をクリックします。

注:ログアウトすると、開いているすべての Virtual KVM Client セッションとシリアル クライアント セッションが閉じられます。

MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定

プロキシ サーバを使用する必要がある場合、リモート クライアント PC 上で SOCKS プロキシを設定する必要があります。

注: インストールされているプロキシ サーバが HTTP プロキシ プロトコルにのみ対応している場合は、接続できません。

SOCKS プロキシを設定するには

1. クライアント上で [コントロール パネル] の [インターネット オプション] を選択します。

a. [接続] タブで [LAN の設定] をクリックします。[ローカル エリア ネットワーク (LAN) の設定] ダイアログ ボックスが開きます。

b. [LAN にプロキシ サーバを使用する] チェック ボックスをオンにします。

c. [詳細] をクリックします。[プロキシの設定] ダイアログ ボックスが開きます。

d. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

2. 各ダイアログ ボックスで [OK] をクリックし、設定内容を適用します。
3. Java™ アプレット用のプロキシを設定するため、[コントロール パネル] の [Java] を選択します。

e. [基本] タブで [ネットワーク設定] をクリックします。[ネットワーク設定] ダイアログ ボックスが開きます。

f. [プロキシ サーバを使用] をクリックします。

g. [詳細] をクリックします。[詳細ネットワーク設定] ダイアログ ボックスが開きます。

h. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

4. スタンドアロン MPC を使用している場合は、次の手順も実行する必要があります。

i. テキスト エディタで、MPC ディレクトリにある start.bat ファイルを開きます。

j. コマンド ラインにパラメータを挿入します。このパラメータは、"-classpath" の前に挿入します。挿入するパラメータは、「-DsocksProxyHost=<SOCKS プロキシ IP アドレス> -DsocksProxyPort=<SOCKS プロキシ ポート番号>」です。

挿入後のコマンドは次のようになります。

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .¥sdeploy.jar;.¥sFoxtrot.jar;.¥jaws.jar;.¥sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC) および Active KVM Client (AKC)

Virtual KVM Client (VKC) および Active KVM Client (AKC) は、リモート ターゲットへのアクセスに使用されるインタフェースです。AKC と VKC は、以下の点を除いて特徴が似ています。

- 最小システム要件
- サポートされているオペレーティング システムとブラウザ
- AKC で作成されたキーボード マクロは、VKC では使用できません。
- ダイレクト ポート アクセス設定 (「**URL を経由したダイレクト ポート アクセスの有効化 『139p. 』**」を参照)
- AKC サーバ証明書検証設定 (「**AKC を使用するための前提条件**」を参照)

Raritan Virtual KVM Client について

リモート コンソールを使用してターゲット サーバにアクセスすると、Virtual KVM Client (VKC) のウィンドウが開かれます。接続されているターゲット サーバごとに 1 つの Virtual KVM Client ウィンドウが表示されます。これらのウィンドウは、Windows® のタスク バーを使用して開くことができます。

注: 一部の機能 (クライアント起動設定、スマート カードなど) は、LX ではサポートされていません。したがって、LX と併用しても AKC や VKC でサポートされません。

注: KX II-101-V2 のみ、一度に 1 台のターゲットへの接続をサポートしています。

Virtual KVM Client ウィンドウは、お使いのコンピュータのデスクトップ上で最小化、最大化、および移動できます。

注: HTML ブラウザ表示を更新すると Virtual KVM Client 接続が切断されてしまうので注意してください。

注: Firefox 3.0.3 を使用している場合は、アプリケーションの起動で問題が発生することがあります。この場合は、ブラウザのキャッシュをクリアして、アプリケーションを再起動してください。

Active KVM Client について

AKC は Microsoft Windows .NET 技術に基づいています。したがって、Raritan の VKC および MPC の実行に必要な Java Runtime Environment (JRE) を使用することなくクライアントを Windows 環境で実行できます。

注: 一部の機能 (クライアント起動設定、スマート カードなど) は、LX ではサポートされていません。したがって、LX と併用しても AKC や VKC でサポートされません。

AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ

.NET Framework

AKC を実行するには .NET® バージョン 3.5 が必要です。AKC は、3.5 と 4.0 の両方がインストールされている状態でも動作しますが、4.0 だけでは動作しません。

オペレーティング システム

AKC を Internet Explorer® から起動することで、KX II 2.2 以降および LX 2.4.5 以降を利用してターゲット サーバに接続できます。AKC は、.NET Framework 3.5 が実行されている以下のプラットフォームに対応しています。

- Windows XP® オペレーティング システム
- Windows Vista® (64 ビット版も可)
- Windows 7® (64 ビット版も可)

AKC を実行するには .NET が必要になるため、.NET がインストールされていない場合、またはサポートされていないバージョンの .NET がインストールされている場合は、.NET バージョンの確認を指示するメッセージが表示されます。

ブラウザ

- Internet Explorer 6 以降

IE 6 以降ではないブラウザから AKC を開こうとすると、ブラウザの確認と Internet Explorer への切り替えを指示するエラー メッセージが表示されます。

AKC を使用するため前提条件

AKC を使用するには、以下の手順に従います。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの［信頼済みサイト］ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

AKC ダウンロード サーバ証明書の検証を有効にする

デバイスの管理者が［AKC ダウンロード サーバ証明書の検証を有効にする］オプションを有効にした場合は、以下の手順に従います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書（または自己署名証明書のコピー）をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

ツールバー

ボタン	ボタン名	説明
	［接続プロパティ］	帯域幅のオプションを（接続スピード、色深度など）を手動で調節するための［接続プロパティの変更］ダイアログ ボックスを開きます。
	［ビデオ設定］	ビデオ変換パラメータを手動で調節するための［ビデオ設定］ダイアログ ボックスを開きます。
	［色調整］	色設定を調節し、余分な色ノイズを低減します。 ［ビデオ］の［色調整］を選択した場合と同じです。 *注: KX II-101-V2 では使用できません。*
	［ターゲット スクリーンショット］	クリックすると、ターゲット サーバのスクリーンショットを取得して、それを選択したファイルに保存します。
	［オーディオ］	クライアント PC に接続されているオーディオ デバイスのリストから選択するためのダイアログ ボックスを開きます。 オーディオ デバイスがターゲットに接続されたら、デバイスを選択して切断します。 *注: この機能は、KX II 2.4.0 以降で利用できます。*

ボタン	ボタン名	説明
		注: この機能は LX ではサポートされていません。
	[マウスの同期]	デュアルマウス モードで、マウス ポインタとターゲット サーバのマウス ポインタを同期させます。 *注: KX II-101-V2 では使用できません。*
	[画面の更新]	ビデオ画面を強制的に更新します。
	[ビデオ設定の自動検出]	ビデオ設定（解像度、垂直走査周波数）を強制的に更新します。
	[スマート カード]	クライアント PC に接続されているスマート カード リーダーのリストから選択するためのダイアログ ボックスを開きます。 *注: この機能は、KSX II 2.3.0 以降および KX II 2.1.10 以降で利用できます。* *注: この機能は LX ではサポートされていません。*
	[Ctrl+Alt+Del の送信]	ターゲット サーバに Ctrl+Alt+Del のキー操作を送信します。
	[シングル カーソル モード]	ローカルのマウス ポインタを画面に表示しない「シングル カーソル モード」になります。 このモードを終了するには、Ctrl+Alt+O キーを押します。 *注: KX II-101-V2 では使用できません。*
	[全画面モード]	ターゲット サーバのデスクトップを表示する画面を最大化します。
	[拡大、縮小]	ターゲットのビデオ サイズを拡大、縮小して、スクロール バーを使用せずにターゲット サーバ ウィンドウの内容をすべて表示できるようにします。

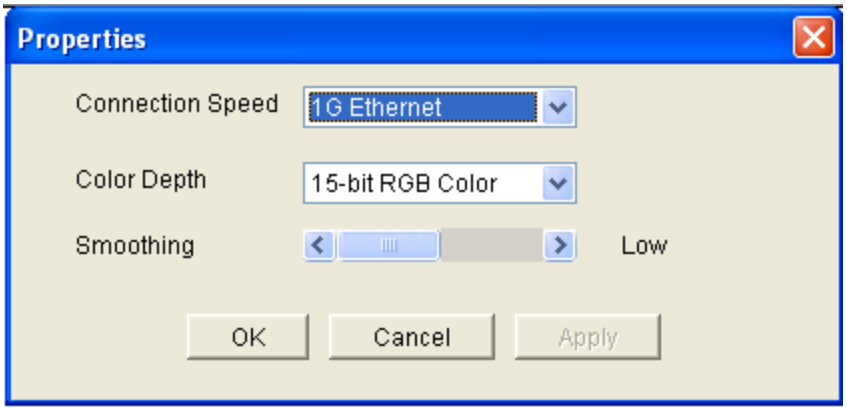
[Connection Properties] (接続プロパティ)

動的ビデオ圧縮アルゴリズムは、さまざまな帯域幅条件で KVM コンソールの使用を可能にします。デバイスの KVM 出力は、LAN 経由だけでなく WAN 経由でも使用できるように最適化されます。さらに、色深度を制御してビデオ出力を制限できるため、さまざまな帯域幅でビデオ画質とシステム応答性のバランスを最適に維持することができます。

[Properties](プロパティ) ダイアログ ボックスのパラメータは、さまざまな動作環境の要件に合わせて最適に設定できます。 接続プロパティは、一度設定して保存すると、それ以降の第 2 世代デバイスへの接続に使用されます。

▶ **接続プロパティを設定するには、以下の手順に従います。**

1. [Connection](接続) の [Properties](プロパティ) を選択するか、ツールバーの [Connection Properties](接続プロパティ) ボタン  をクリックします。[Properties](プロパティ) ダイアログ ボックスが表示されます。



注:KX II-101 は 1G Ethernet をサポートしていません。

2. ドロップダウン リストから接続スピードを選択します。デバイスでは、使用可能な帯域幅を自動的に検出できるため、帯域幅利用は制限されません。ただし、帯域幅の制限に応じて帯域幅利用を調整することもできます。
   - 自動
   - [1G Ethernet] (1G Ethernet)
   - [100 Mb Ethernet] (10 Mbps Ethernet)
   - [10 Mb Ethernet] (10 Mbps Ethernet)
   - [1.5 Mb (MAX DSL/T1)] (1.5 Mbps (最高速 DSL/T1))
   - [1 Mb (Fast DSL/T1)] (1 Mbps (高速 DSL/T1))
   - [512 Kb (Medium DSL/T1)] (512 Kbps (中速 DSL/T1))

- [384 Kb (Slow DSL/T1)] (384 Kbps (低速 DSL/T1))
- [256 Kb (Cable)] (256 Kbps (ケーブル))
- [128 Kb (Dual ISDN)] (128 Kbps (デュアル ISDN))
- [56 kb (ISP Modem)] (56 Kbps (ISP モデム))
- [33 kb (Fast Modem)] (33 Kbps (高速モデム))
- [24 kb (Slow Modem)] (24 Kbps (低速モデム))

これらの設定は、実際の速度ではなく特定の条件に対して最適化されています。クライアントおよびサーバは、現在のネットワーク速度やエンコード設定に関係なく、常に最高速度でネットワークにビデオを配信しようとします。ただし、システムの応答性が最も高くなるのは、設定が実際の環境と一致するときだけです。

3. ドロップダウン リストから色深度を選択します。デバイスでは、リモート ユーザに送信される色深度を動的に調整することで、さまざまな帯域幅で最適な使いやすさを実現します。
   - [15-bit RGB Color] (8 ビット RGB カラー)
   - [8-bit RGB Color] (8 ビット RGB カラー)
   - [4-bit Color] (4 ビット カラー)
   - [4-bit Gray] (2 ビット グレー)
   - [3-bit Gray] (2 ビット グレー)
   - [2-bit Gray] (2 ビット グレー)
   - [Black and White] (モノクロ)

   重要: 多くの管理タスク (サーバの監視、再設定等) において、最新のビデオ グラフィック カードのほとんどで利用できる 24 ビットまたは 32 ビットのフルカラー表示は必要ありません。このような高い色深度を送信すると、ネットワークの帯域幅を浪費することになります。
4. スライダを使用して、スムージングのレベルを指定します (15 ビット カラー モードのみ)。ここで設定したスムージングのレベルにより、色がわずかに異なる画面領域をできるだけ滑らかな単色の組み合わせにするかが決まります。スムージングにより、表示されるビデオ ノイズを軽減することで、対象ビデオの画質が向上します。
5. [OK] をクリックして、これらのプロパティを保存します。

接続情報

Virtual KVM Client 接続に関する情報を取得するには、以下の手順に従います。

- [Connection] (接続) の [Info...] (情報...) を選択します。[Connection Info] (接続情報) ウィンドウが開きます。

現在の接続に関する以下の情報が表示されます。

- [Device Name] (デバイス名) – デバイスの名前です。
- [IP Address] (IP アドレス) – デバイスの IP アドレスです。
- [Port] (ポート) – ターゲット デバイスへのアクセスに使用される KVM 通信 TCP/IP ポートです。
- [Data In/Second] (データ入力/秒) – 入力データ レートです。
- [Data Out/Second] (データ出力/秒) – 出力データ レートです。
- [Connect Time] (接続時間) – 接続時間です。
- [FPS] (FPS) – ビデオで送信される毎秒フレーム数です。
- [Horizontal Resolution] (水平解像度) – 水平方向の画面解像度です。
- [Vertical Resolution] (垂直解像度) – 垂直方向の画面解像度です。
- [Refresh Rate] (垂直走査周波数) – 画面の更新頻度を表します。
- [Protocol Version] (プロトコル バージョン) – RFB プロトコル バージョンです。

この情報をコピーするには、以下の手順に従います。

- [Copy to Clipboard] (クリップボードにコピー) をクリックします。これにより、任意のプログラムにこの情報を貼り付けることができます。

キーボードのオプション

[Keyboard Macros] (キーボード マクロ)

キーボード マクロを利用することで、ターゲット サーバに対するキー入力が確実にターゲット サーバに送信され、ターゲット サーバのみで解釈されます。キーボード マクロを利用しない場合、Virtual KVM Client が実行されているコンピュータ（クライアント PC）によって解釈される可能性があります。

マクロはクライアント PC に保存され、その PC 専用になります。したがって、別の PC を使用したときは、作成したマクロを使用できません。さらに、キーボード マクロはコンピュータ単位で管理されるので、あるユーザが使用している PC に別のユーザが自分の名前でログインした場合でも、1 人目のユーザが作成したマクロが 2 人目のユーザに対して表示されます。

Virtual KVM Client 内で作成したキーボード マクロは Multi-Platform Client (MPC) で使用でき、またその逆も可能です。ただし、Active KVM Client (AKC) で作成したキーボード マクロは、VKC または MPC で使用できません。また、その逆でも使用できません。

注:KX II-101 は AKC をサポートしていません。

キーボード マクロのインポート/エクスポート

Active KVM Client (AKC) からエクスポートされるマクロは、Multi-Platform Client (MPC) および Virtual KVM Client (VKC) にはインポートできません。MPC または VKC からエクスポートされるマクロは、AKC にはインポートできません。

注:KX II-101 は AKC をサポートしていません。

▶ **マクロをインポートするには、以下の手順に従います。**

1. [Keyboard] (キーボード) の [Import Keyboard Macros] (キーボード マクロのインポート) をクリックして、[Import Macros] (マクロのインポート) ダイアログ ボックスを開きます。マクロ ファイルがあるフォルダに移動します。
2. マクロ ファイルをクリックし、[Open] (開く) をクリックしてマクロをインポートします。
   a. ファイル内のマクロ数が多い場合は、エラー メッセージが表示され、[OK] を選択するとインポートが中断されます。
   b. インポートが失敗した場合は、エラー ダイアログ ボックスが表示され、失敗した理由についてのメッセージが表示されます。[OK] をクリックすると、インポートできなかったマクロをスキップしてインポートが続行されます。

3. インポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All]（すべて選択）または [Deselect All]（すべて選択解除）オプションを使用して選択します。
4. [OK] をクリックしてインポートを開始します。
   a. 重複するマクロが見つかった場合は、[Import Macros]（マクロのインポート）ダイアログ ボックスが表示されます。以下のいずれかの手順に従います。
      - [Yes]（はい）をクリックして、既存のマクロを、インポートしたマクロで置き換えます。
      - [Yes to All]（すべてはい）をクリックして、現在選択されているマクロとその他に見つかった重複マクロすべてを置き換えます。
      - [No]（いいえ）をクリックすると、元のマクロが維持され、次のマクロに進みます。
      - [No to All]（すべていいえ）をクリックすると、元のマクロが維持され、次のマクロに進みます。その他に見つかったすべての重複マクロも同様にスキップされます。
      - [Cancel]（キャンセル）をクリックすると、インポートが終了します。
      - または、[Rename]（名前変更）をクリックして、マクロの名前を変更してそれをインポートします。[Rename]（名前変更）が選択された場合は、[Rename Macro]（マクロ名の変更）ダイアログ ボックスが表示されます。フィールドに新しいマクロ名を入力し、[OK] をクリックします。ダイアログ ボックスが閉じられ、処理が続行されます。入力した名前が別のマクロと重複している場合は、アラートが表示されるので、別のマクロ名を入力する必要があります。
   b. インポート処理中にインポート済みマクロの許容数を超えた場合は、ダイアログ ボックスが表示されます。[OK] をクリックして、マクロのインポート試行を続行するか、[Cancel]（キャンセル）をクリックしてインポート処理を中止します。

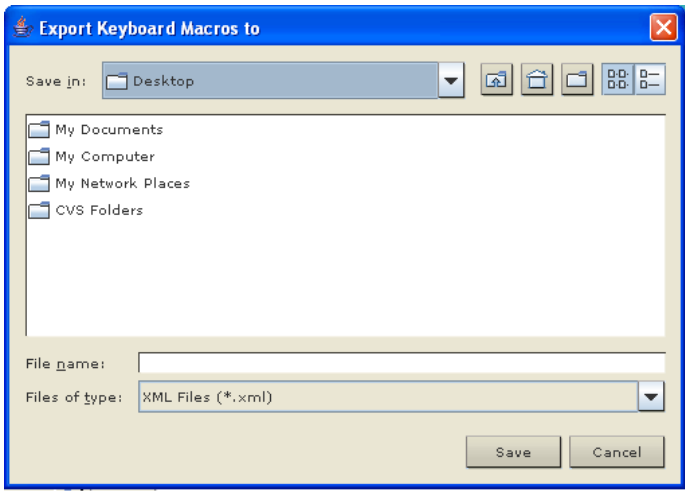
これでマクロがインポートされます。既に存在するホットキーを含むマクロがインポートされた場合、インポートされたマクロのホットキーが破棄されます。

マクロをエクスポートするには、以下の手順に従います。

1. [Tools] (ツール) の [Export Macros] (マクロのエクスポート) を選択して、[Select Keyboard Macros to Export] (エクスポートするキーボード マクロの選択) ダイアログ ボックスをクリックします。

2. エクスポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All] (すべて選択) または [Deselect All] (すべて選択解除) オプションを使用して選択します。
3. [OK] (OK) をクリックします。マクロ ファイルの検索と選択を行うためのダイアログ ボックスが表示されます。デフォルトでは、マクロはデスクトップにあります。

4. マクロ ファイルを保存するフォルダを選択し、ファイル名を入力し、[Save] (保存) をクリックします。マクロが既に存在する場合は、警告メッセージが表示されます。[Yes] (はい) を選択して既存のマクロを上書きするか、[No] (いいえ) をクリックしてマクロを上書きせずに警告を閉じます。



キーボード マクロの作成

▶ マクロを作成するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) をクリックします。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. [Add] (追加) をクリックします。[Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスが表示されます。
3. [Keyboard Macro Name] (キーボード マクロ名) フィールドにマクロの名前を入力します。この名前は、マクロの作成後に [Keyboard] (キーボード) メニューに表示されます。
4. [Hot-Key Combination] (ホットキーの組み合わせ) フィールドで、ドロップダウン リストからキー操作の組み合わせを選択します。これにより、定義済みのキー入力を使用してマクロを実行できます。**オプション**
5. [Keys to Press] (押すキー) ドロップダウン リストで、コマンドの実行用のキー入力をエミュレートするための各キーを選択します。押される順にキーを選択します。各キーの選択後に、[Add Key] (キーの追加) を選択します。選択した各キーは、[Macro Sequence] (マクロ シーケンス) フィールドに表示され、選択するたびに [Release Key] (キーをリリース) コマンドが自動的に追加されます。
6. マクロの [Send Text to Target] (テキストをターゲットに送信) 機能を使用するには、[Construct Macro from Text] (テキストからマクロを作成) ボタンをクリックします。

7. たとえば、左 Ctrl +Esc を選択して、ウィンドウを閉じるマクロを作成します。このマクロは、[Macro Sequence] (マクロ シーケンス) ボックスに次のように表示されます。

   [Press Left Ctrl] (左 Ctrl を押す)

   [Release Left Ctrl] (左 Ctrl をリリースする)

   [Press Esc] (Esc を押す)

   [Release Esc] (左 Esc をリリースする)

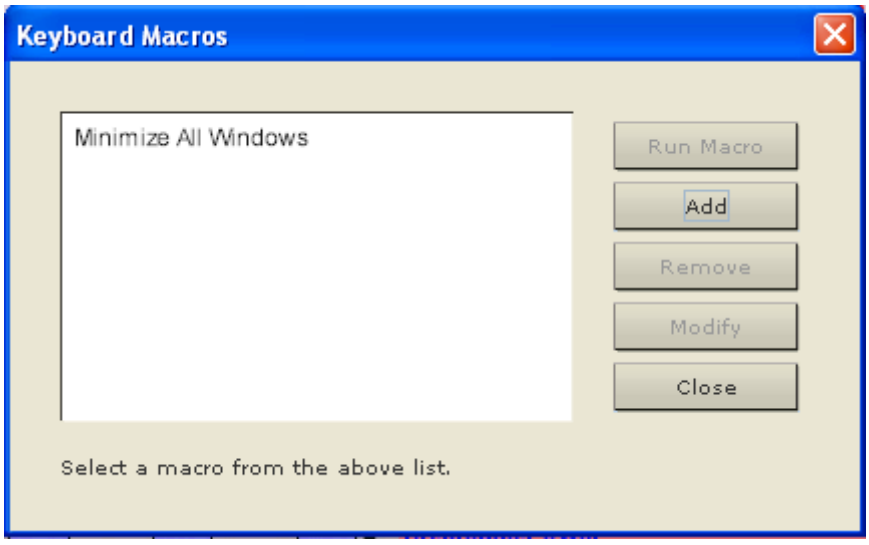
8. [Macro Sequence] (マクロ シーケンス) フィールドで、マクロ シーケンスが正しく定義されていることを確認します。

   a. キー操作の 1 つの手順を削除するには、手順を選択して [Remove] (削除) をクリックします。

   b. キー操作の手順の順番を変更するには、手順をクリックし、必要に応じて上/下の矢印ボタンをクリックして順序を変更します。

9. [OK] をクリックしてマクロを保存します。[クリア] をクリックすると、すべてのフィールドがクリアされ、最初の状態に戻ります。[OK] をクリックすると [Keyboard Macros] (キーボード マクロ) ウィンドウが表示され、新しいキーボード マクロのリストが表示されます。

10. [Close] (閉じる) をクリックして [Keyboard Macro] (キーボード マクロ) ダイアログ ボックスを閉じます。これで、アプリケーションの [Keyboard] (キーボード) メニューにマクロが表示されます。メニューの新しいマクロを選択して実行するか、マクロに割り当てたキー入力を使用します。



キーボード マクロの実行

作成したキーボード マクロは、割り当てたキーボード マクロを使用するか、[Keyboard](キーボード) メニューからそれを選択して起動します。

メニュー バーからのマクロの実行

マクロを作成すると、そのマクロが [Keyboard](キーボード) メニューに表示されます。キーボード マクロを実行するには、[Keyboard](キーボード) メニューでそれをクリックします。

キー操作の組み合わせを使用したマクロの実行

マクロの作成時にキー操作の組み合わせを割り当てた場合は、割り当てたキー入力を押すことでマクロを実行できます。たとえば、Ctrl+Alt+0 キーを同時に押すと、Windows ターゲット サーバの全ウィンドウが最小化されます。

キーボード マクロの変更および削除

▶ マクロを変更するには、以下の手順に従います。

1. [Keyboard](キーボード) の [Keyboard Macros](キーボード マクロ) を選択します。[Keyboard Macros](キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Modify](変更) をクリックします。[Add/Edit Keyboard Macro](キーボード マクロの追加/編集) ダイアログ ボックスが表示されます。
4. 必要な変更を加えます。
5. [OK](OK) をクリックします。

▶ マクロを削除するには、以下の手順に従います。

1. [Keyboard](キーボード) の [Keyboard Macros](キーボード マクロ) を選択します。[Keyboard Macros](キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Remove](削除) をクリックします。マクロが削除されます。

Ctrl+Alt+Del マクロ

Ctrl+Alt+Delete マクロは、頻繁に使用されるため事前にプログラムされています。ツール バーの [Ctrl+Alt+Delete] ボタン 

をクリックすると、現在接続中のサーバまたは KVM スイッチにこのキー操作が送信されます。

一方、Ctrl キー、Alt キー、Delete キーを同時に押すと、Windows オペレーティング システムの構造により、コマンドはターゲット サーバへ送信されずに操作中の PC に適用されます。

CIM キーボード/マウス オプションの設定

▶ **DCIM-USBG2 の設定メニューにアクセスするには、以下の手順に従います。**

1. Windows® のメモ帳などのウィンドウにマウス ポインタを置きます。
2. [Set CIM Keyboard/Mouse options] (CIM キーボード/マウス オプションを設定する) を選択します。この操作は、左 Ctrl + Num Lock キーをターゲットに送信することと同じです。CIM セットアップ メニュー オプションが表示されます。
3. 言語とマウスを設定します。
4. メニューを終了し、通常の CIM 機能に戻ります。

ビデオのプロパティ

画面を更新する

[Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。ビデオの設定を自動的に更新する方法はいくつかあります。

- [Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。
- [Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ターゲット サーバのビデオ設定が自動的に検出されます。
- [Calibrate Color] (色調整) コマンドを使用すると、ビデオの表示色が調整されます。

これに加え、[Video Settings] (ビデオ設定) コマンドを使用すると、手動で設定を調整できます。

▶ **ビデオ設定を更新するには、次のいずれかの手順に従います。**

- [Video] (ビデオ) の [Refresh Screen] (画面の更新) を選択するか、ツールバーの [Refresh Screen] (画面の更新) ボタン  をクリックします。

[Auto-sense Video Settings] (ビデオ設定の自動感知)

[Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ビデオ設定 (解像度、垂直走査周波数) が再検出され、ビデオ画面が再描画されます。

▶ **ビデオ設定を自動的に検出するには、以下の手順に従います。**

- [Video] (ビデオ) の [Auto-sense Video Settings] (ビデオ設定の自動検出) を選択するか、ツールバーの [Auto-sense Video Settings] (ビデオ設定の自動検出) ボタン  をクリックします。調整が行われていることを示すメッセージが表示されます。

色の調整

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、輝度、彩度) を最適化するために使用します。色設定は、ターゲット サーバごとに適用されます。

注: [Calibrate Color] (色調整) コマンドは、現在の接続のみに適用されます。

注: KX II-101 では、色の調整はサポートされません。

▶ **色を調整するには、以下の手順に従います。**

- [Video] (ビデオ) の [Calibrate Color] (色調整) を選択するか、ツールバーの [Calibrate Color] (色調整) ボタン  をクリックします。ターゲット デバイス画面の色が調整されます。

ビデオ設定を調整する

[Video Settings] (ビデオ設定) コマンドを使用すると、ビデオ設定を手動で調整できます。

▶ **ビデオ設定を変更するには、以下の手順に従います。**

1. [Video] (ビデオ) の [Video Settings] (ビデオ設定) を選択するか、ツールバーの [Video Settings] (ビデオ設定) ボタン  をクリックして、[Video Settings] (ビデオ設定) ダイアログ ボックスを開きます。
2. 必要に応じて、以下の設定を調整します。設定を調整すると、その効果が即座に表示に反映されます。
   a. [Noise Filter] (ノイズ フィルタ)

デバイスでは、グラフィック カードからのビデオ出力の電気的干渉を除去することができます。この機能により、画質が最適化され、消費される帯域幅が低減されます。設定値を大きくすると、ピクセル変動は隣接するピクセルと比較して大きな色変化がある場合にのみ送信されます。ただし、しきい値を高く設定しすぎると、正常な画面変更が意図せずフィルタリングされてしまう場合があります。
設定値を低くすると、ほとんどのピクセルの変更が送信されます。しきい値を低く設定しすぎると、帯域幅の使用量が高くなることがあります。

b. [PLL Settings] (PLL 設定)

[Clock] (クロック) – ビデオ画面上にビデオ ピクセルが表示される速度を制御します。クロック設定値を変更すると、ビデオ画像が水平方向に伸縮します。設定値は奇数を推奨します。通常は自動検出機能によって適切に設定されるため、ほとんどの環境ではこの設定を変更する必要はありません。

[Phase] (位相) – 位相の値の範囲は 0 ～ 31 です。これより大きな値は反復されます。アクティブなターゲット サーバ用に最適なビデオ画像が得られる位相の位置で停止してください。

c. [Brightness] (明るさ): この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。

d. [Brightness Red] (赤輝度) – ターゲット サーバの画面に表示される赤の信号の輝度を制御します。

e. [Brightness Green] (緑輝度) – 緑の信号の輝度を制御します。

f. [Brightness Blue] (青輝度) – 青の信号の輝度を制御します。

g. [Contrast Red] (赤コントラスト) – 赤の信号のコントラストを制御します。

h. [Contrast Green] (緑コントラスト) – 緑の信号のコントラストを制御します。

i. [Contrast Blue] (青コントラスト) – 青の信号のコントラストを制御します。

ビデオ画像が大幅にぼやけている場合、設定でクロックと位相を調節することで、アクティブなターゲット サーバの画像を改善します。

警告: クロック設定と位相設定を変更する際には、注意が必要です。ビデオ画像が消えたり歪んだりする可能性があるだけでなく、元の状態に戻せなくなることがあります。変更を加える前に、ラリタン テクニカル サポートにお問い合わせください。

---

j. [Horizontal Offset] (水平オフセット) – ターゲット サーバの画面がモニタに表示されるときの水平位置を制御します。

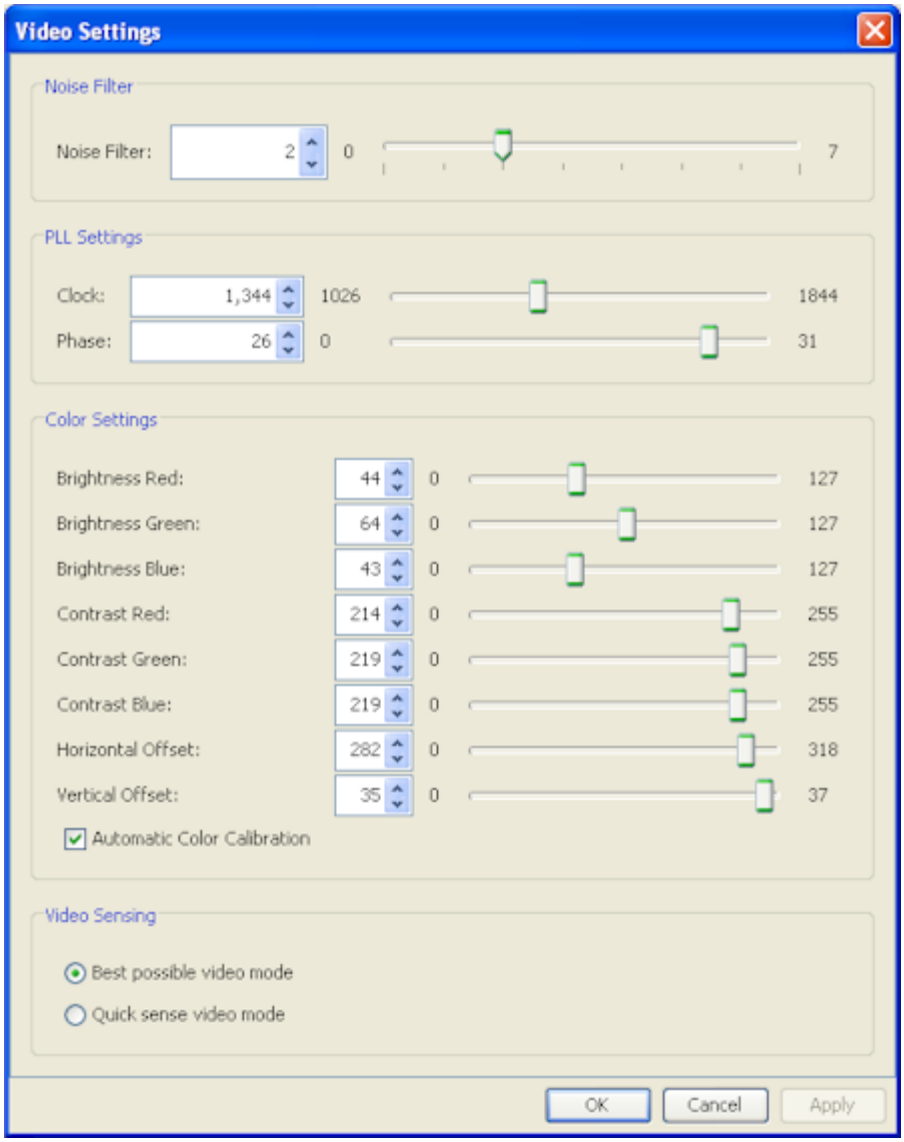
k. [Vertical Offset]（垂直オフセット）- ターゲット サーバの画面がモニタに表示されるときの垂直位置を制御します。

3. [Automatic Color Calibration]（自動色調節）を選択して、この機能を有効にします。
4. ビデオ検出モードを選択します。
   - [Best possible video mode]（最適ビデオ モード）

   ターゲットやターゲットの解像度が変更されたときに、すべての自動検出処理が実行されます。このオプションを選択すると、最適な画像品質になるようにビデオが調整されます。
   - [Quick sense video mode]（クイック検出ビデオ モード）

   このオプションを使用すると、クイック ビデオ自動検出が使用され、ターゲットのビデオがより早く表示されます。このオプションは、再起動直後のターゲット サーバの BIOS 設定を入力するときに特に有効です。
5. 設定を適用してダイアログ ボックスを閉じるには、[OK] をクリックします。ダイアログ ボックスを閉じずに設定を適用するには、[Apply]（適用）をクリックします。

注: 一部の Sun サーバでは、ある種の Sun 背景画面 (外周部が非常に暗いものなど) が中央の位置に正確に表示されない場合があります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

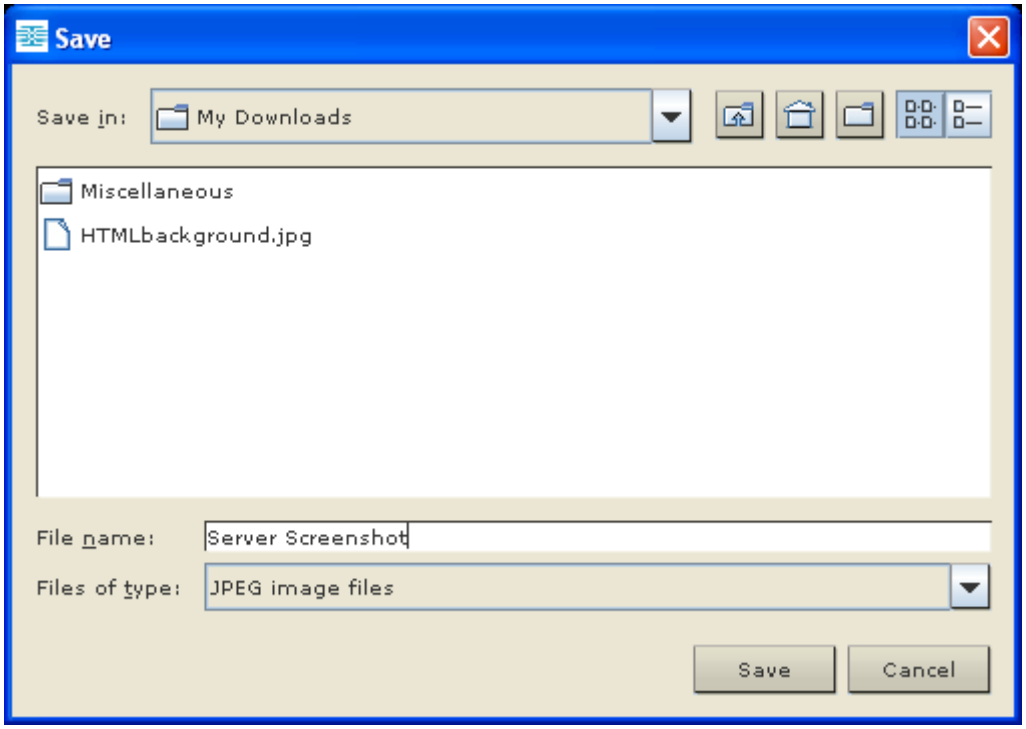


[Screenshot from Target] (ターゲットからのスクリーンショット) を使用する

[Screenshot from Target] (ターゲットからのスクリーンショット) サーバ コマンドを使用してターゲット サーバのスクリーンショットを撮ることができます。必要に応じて、選択した場所にこのスクリーンショットをビットマップ、JPEG、または PNG ファイルとして保存します。

▶ **ターゲット サーバのスクリーンショットを撮るには、次の手順に従います。**

1. [Video] (ビデオ) の [Screenshot from Target] (ターゲットからのスクリーンショット) を選択するか、ツールバーの [Screenshot from Target] (ターゲットからのスクリーンショット) ボタン  をクリックします。
2. [Save] (保存) ダイアログ ボックスで、ファイルの保存場所を選択し、ファイルに名前を付けて、[Files of type] (ファイルの種類) ドロップダウンからファイル形式を選択します。
3. [Save] (保存) をクリックしてスクリーンショットを保存します。



最大垂直走査周波数の変更

ターゲットで使用しているビデオ カードでカスタム ソフトウェアが使用されている場合、MPC または VKC を介してターゲットにアクセスするには、垂直走査周波数がターゲットで有効になるように、モニタの最大垂直走査周波数を変更する必要があります。

▶ **モニタの垂直走査周波数を調整するには、以下の手順に従います。**

1. Windows® では、[画面のプロパティ] ダイアログ ボックスを開き、[設定]、[詳細設定] の順に選択してプラグ アンド プレイのダイアログ ボックスを開きます。
2. [モニタ] タブをクリックします。
3. [画面のリフレッシュ レート] を設定します。
4. [OK] をクリックし、もう一度 [OK] をクリックして設定を適用します。

マウス オプション

ターゲット サーバを制御しているとき、リモート コンソールには、2 つのマウス カーソルが表示されます。1 つはクライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。

この場合、シングル マウス モードとデュアル マウス モードのどちらかを使用できます。デュアル マウス モードで、オプションが正しく設定されている場合は、2 つのマウス カーソルが同調します。

デバイスでは、2 つのマウス カーソルが存在するときに以下のマウス モードが提供されます。

- 絶対 (マウス同期)
- インテリジェント (マウス モード)
- 標準 (マウス モード)

マウス ポインタの同期

マウスが使用されているターゲット サーバをリモートで表示する場合、2 つのマウス カーソルが表示されます。1 つはリモート クライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。マウス ポインタが Virtual KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。

高速 LAN 接続の場合、Virtual KVM Client のマウス ポインタを無効にしてターゲット サーバのマウス ポインタのみを表示できます。この 2 つのモード（シングル マウスとデュアル マウス）は自由に切り替えることができます。

マウス同期のヒント

マウスの同期を設定するには、以下の手順に従います。

1. 選択したビデオ解像度と垂直走査周波数がデバイスでサポートされていることを確認します。[Virtual KVM Client 接続情報] ダイアログ ボックスには、デバイスの表示で使用している実際の値が表示されます。
2. KX II デバイスおよび LX デバイスの場合は、ケーブルの長さが選択したビデオ解像度に指定されている限度内であることを確認します。
3. インストール プロセス中にマウスとビデオが正しく構成されていることを確認します。
4. [Virtual KVM Client の自動検出] ボタンをクリックして自動検出を強制します。
5. 以上の手順で Linux、UNIX、Solaris KVM ターゲット サーバのマウス同期が改善しない場合は、以下の手順に従います。
   a. ターミナル ウィンドウを開きます。
   b. コマンド「`xset mouse 1 1`」を入力します。
   c. ターミナル ウィンドウを閉じます。
6. [Virtual KVM Client マウス同期] ボタン  をクリックします。

インテリジェント マウス モードでの追加の注意事項

- 同期ルーチンが利用する領域を空けるため、画面の左上隅にアイコンやアプリケーションがないことを確認します。
- アニメーション カーソルを使用しないでください。
- KVM ターゲット サーバでアクティブなデスクトップを無効にします。

マウスの同期

デュアル マウス モードで [Synchronize Mouse] (マウスの同期) コマンドを使用すると、ターゲット サーバのマウス ポインタと Virtual KVM Client のマウス ポインタとの同期化が再実行されます。

▶ **マウスを同期するには、次のいずれかの手順に従います。**

- [Mouse] (マウス) の [Synchronize Mouse] (マウスの同期) を選択するか、ツールバーの [Synchronize Mouse] (マウスの同期) ボタン をクリックします。

注: このオプションは、標準マウス モードとインテリジェント マウス モードでのみ使用可能です。

標準マウス モード

標準マウス モードは、相対マウス位置を使用した標準のマウス同期アルゴリズムです。標準マウス モードを使用する場合、クライアントとサーバのカーソルが同期するように、マウスの加速を無効にし、マウスに関連するその他のパラメータを適切に設定する必要があります。

▶ **標準マウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Standard] (標準) を選択します。

インテリジェント マウス モード

デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス設定を検出し、それに応じてマウス カーソルを同期できるので、ターゲットでマウスの加速を設定できます。インテリジェント マウス モードは、VM ターゲット以外のデフォルトです。

同期中は、マウス カーソルが画面の左上隅で ″ダンス″ をし、加速が計算されます。このモードが正常に動作するには、特定の条件が満たされる必要があります。

▶ インテリジェント マウス モードに切り替えるには、以下の手順に従います。

- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

[Mouse] (マウス) メニューにある [Intelligent Mouse Synchronization] (インテリジェント マウス同期) コマンドを選択すると、マウスが動いていないときにマウス カーソルが自動的に同期されます。この機能を適切に動作させるには、次の条件が満たされている必要があります。

- ターゲットにおいて、アクティブ デスクトップが無効であること。
- ターゲット ページの左上隅にウィンドウが表示されていないこと。
- ターゲット ページの左上隅にアニメーション背景が表示されていないこと。
- ターゲットのマウス カーソルが通常のものであり、アニメーション カーソルでないこと。
- ターゲット マウスの速度が、非常に遅い値や非常に速い値に設定されていないこと。
- [ポインタの精度を高める] や [ポインタを自動的に既定のボタン上に移動する] などの高度なマウス プロパティが無効であること。
- [ビデオ設定] ウィンドウで [最適ビデオ モード] を選択していること。
- ターゲットのビデオの外周部が明確に表示されていること (つまり、ターゲットのビデオ画像の端にスクロールしたときに、ターゲット デスクトップとリモート KVM コンソール ウィンドウの間に黒いボーダーが表示されている必要があります)。
- インテリジェント マウス同期機能を使用中に、デスクトップの左上隅にファイル アイコンやフォルダ アイコンがあると、この機能が正しく動作しない可能性があります。この機能での問題を避けるために、デスクトップの左上隅にファイル アイコンやフォルダ アイコンを置かないことを推奨します。

ターゲット ビデオが自動検出された後で、ツール バーの [Synchronize Mouse] (マウス同期) ボタンをクリックして、手動でマウス同期を開始する必要があります。ターゲットの解像度が変更された場合や、マウス カーソルが互いに同期しなくなった場合にも、この操作を行います。

インテリジェント マウス同期が失敗した場合、標準マウス同期と同じ動作になります。

マウス設定は、ターゲットのオペレーション システムよって異なります。詳細については、使用する OS のマニュアルを参照してください。また、インテリジェント マウス同期は UNIX ターゲットでは機能しません。

ずれないマウス モード

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのカーソルを同期するために絶対座標が使用されます。このモードは USB ポートを備えたサーバでサポートされ、VM およびデュアル VM ターゲットではデフォルトのモードです。

▶ **ずれないマウス モードに切り替えるには、以下の手順に従います。**

- [Mouse]（マウス）の [Absolute]（ずれない）を選択します。

注: LX では、ずれないマウス機能は、仮想メディアに対応する USB CIM (D2CIM-VUSB および D2CIM-DVUSB) でのみ使用できます。

シングル マウス モード

シングル マウス モードでは、ターゲット サーバのマウス カーソルだけを使用します。ローカル マウス ポインタは画面に表示されません。シングル マウス モードでは、[マウスの同期] コマンドは使用できません（単独のマウス カーソルを同期化する必要がないため）。

注: VM をクライアントとして使用する場合、シングル マウス モードは Windows ターゲットや Linux ターゲットでは機能しません。

▶ **シングル マウス モードに入るには、以下の手順に従います。**

1. [Mouse]（マウス）の [Single Mouse Cursor]（シングル マウス カーソル）を選択します。

2. ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カーソル) ボタン をクリックします。

▶ シングル マウス モードを終了するには、以下の手順に従います。

- シングル マウス モードを終了するには、キーボードの Ctrl+Alt+O を押します。

ツール オプション

[全般]

▶ ツール オプションを設定するには、以下の手順に従います。

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. テクニカル サポートから指示されたときだけ、[ログ記録を有効にする] チェックボックスをオンにします。このオプションをオンにすると、ホーム ディレクトリにログ ファイルが作成されます。
3. 必要に応じて、ドロップダウン リストからキーボードの種類を選択します。含まれるオプションは次のとおりです。
   - [アメリカ英語/インターナショナル]
   - [フランス語 (フランス)]
   - [ドイツ語 (ドイツ)]
   - [日本語]
   - [イギリス英語]
   - [韓国語 (韓国)]
   - [フランス語 (ベルギー)]
   - [ノルウェー語 (ノルウェー)]
   - [ポルトガル語 (ポルトガル)]
   - [デンマーク語 (デンマーク)]

- [スウェーデン語 (スウェーデン)]
- [ドイツ語 (スイス)]
- [ハンガリー語 (ハンガリー)]
- [スペイン語 (スペイン)]
- [イタリア語 (イタリア)]
- [スロベニア語]
- [変換: フランス語 – アメリカ英語]
- [変換: フランス語 – アメリカ英語/インターナショナル]

AKC では、デフォルトのキーボードの種類はローカル クライアントであるため、このオプションは適用されません。また、KX II-101 および KX II-101-V2 は、シングル カーソル モードをサポートしていないので、これらのデバイスには [シングル カーソル モードの終了] 機能は適用されません。

4. ホットキーを設定します。
   - [全画面モードの終了 – ホットキー]: 全画面モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。これは、このモードを終了するためのホットキーです。
   - [シングル カーソル モードの終了- ホットキー]: シングル カーソル モードに入ると、ターゲット サーバのマウス カーソルのみが表示されます。これは、シングル カーソル モードを終了して、クライアント マウス カーソルに戻るために使用するホットキーです。
   - [ターゲットから切断 – ホットキー]: このホットキーを有効にすると、ターゲットからすばやく切断できます。

   アプリケーションでは、同じホットキーの組み合わせを複数の機能に割り当てることはできません。たとえば、Q が既に [ターゲットから切断] 機能に割り当てられている場合、それを [全画面モードの終了] 機能に割り当てることはできません。さらに、ホットキーがアップグレードによってアプリケーションに追加されたときにそのキーのデータ値が既に使用されていた場合は、次に利用できる値が、代わりにその機能に適用されます。
5. [OK] をクリックします。

キーボードの制限

トルコ語キーボード

トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

スロベニア語キーボード

JRE の制限により、< キーは、スロベニア語キーボードでは機能しません。

Linux での言語設定

Linux 上の Sun JRE では、システムの環境設定を使用して設定される外国語のキーボードで正しいキー イベントを生成する際に問題があるので、外国語キーボードは、次の表で説明する方法を使用して設定することをお勧めします。

言語	設定方法
アメリカ英語/国際	デフォルト設定
フランス語	Keyboard Indicator
ドイツ語	[System Settings] (システム設定) (Control Center)
日本語	[System Settings] (システム設定) (Control Center)
イギリス英語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control Center)
ベルギー語	Keyboard Indicator
ノルウェー語	Keyboard Indicator
デンマーク語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

クライアント起動設定

LX ユーザは、クライアント起動設定をカスタマイズし、KVM セッションにおける画面設定を定義できます。

注: この機能は、MPC では利用できますが、AKC および VKC では利用できません。

▶ クライアント起動設定をカスタマイズするには、以下の手順に従います。

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. [クライアント起動設定] タブをクリックします。
   - ターゲット ウィンドウ設定をカスタマイズするには、以下の手順に従います。
   a. ターゲットの現在の解像度に合ったサイズのウィンドウを開くには、[標準 – ターゲットの解像度に合わせる] を選択します。ターゲットの解像度がクライアントの解像度よりも高い場合、画面全体にターゲット ウィンドウが表示され、表示しきれない部分がある場合は、スクロール バーが追加表示されます。
   b. ターゲット ウィンドウを全画面モードで開くには、[全画面] を選択します。
   - ターゲット ビューアが起動するモニタをカスタマイズするには
   a. クライアント上で使用されているアプリケーション (例: Web ブラウザ、アプレット) を表示しているモニタと同じモニタを使用してターゲット ビューアを起動するには、[クライアントが起動されているモニタ] を選択します。
   b. アプリケーションによって現在検出されているモニタの一覧から選択するには、[検出されたモニタの中から選択] を選択します。以前選択したモニタが検出されなくなった場合、"現在選択されているモニタは検出されませんでした" というメッセージが表示されます。
   - 追加の起動設定をカスタマイズするには、以下の手順に従います。
   a. サーバにアクセスされたときにデフォルト マウス モードとしてシングル マウス モードを有効にするには、[シングル カーソル モードを有効にする] を選択します。
   b. ターゲット サーバにアクセスされたときに、ディスプレイのサイズを自動的に拡大、縮小するには、[ビデオの拡大、縮小を有効にする] 選択します。

c. 全画面モードの場合でもターゲットのツールバーを表示したままにする場合は、[メニュー ツールバーを常に表示] を選択します。デフォルトでは、ターゲットが全画面モードの場合、メニューは、マウスを画面上部に移動した場合にのみ表示されます。

3. [OK] をクリックします。

スキャン設定

LX には、選択したターゲットを検索してそれをスライド ショー ビューで表示するポート スキャン機能が用意されています。これを使用すると、最大 32 のターゲットを一度にモニタできます。ターゲットに接続することも、必要に応じて特定のターゲットをフォーカスすることもできます。スキャン対象は、標準ターゲット、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。 「*ポートのスキャン 『48p. 』*」を参照してください。[スキャン設定] タブを使用して、スキャン間隔およびデフォルト表示オプションをカスタマイズします。

▶ **スキャン設定をカスタマイズするには、以下の手順に従います。**

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. [スキャン設定] タブを選択します。
3. [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
4. [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
5. [表示] セクションで、[ポート スキャン] ウィンドウのサムネイルのサイズと分割方向のデフォルト表示オプションを変更します。
6. [OK] をクリックします。

表示オプション

[View Toolbar] (ツール バーの表示)

Virtual KVM Client では、ツール バーの表示/非表示を切り替えることができます。

▶ **ツール バーの表示/非表示 (オン/オフ) を切り替えるには、以下の手順に従います。**

- [View] (表示) の [View Toolbar] (ツール バーの表示) を選択します。

[View Status Bar] (ステータス バーの表示)

デフォルトでは、ステータス バーはターゲット ウィンドウの下部に表示されます。

▶ **ステータス バーを非表示にするには、以下の手順に従います。**

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択解除します。

▶ **ステータス バーを復元するには、以下の手順に従います。**

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択します。

[Scaling] (拡大、縮小)

ターゲットのウィンドウを拡大、縮小することで、ターゲット サーバ ウィンドウ全体の内容を表示することができます。Virtual KVM Client のウィンドウ サイズに合わせて、縦横比を維持したまま、ターゲット ビデオのサイズを拡大または縮小することができるため、スクロール バーを使用することなくターゲット サーバのデスクトップ全体を表示することができます。

▶ **拡大、縮小 (オン/オフ) を切り替えるには、以下の手順に従います。**

- [View] (表示) の [Scaling] (拡大、縮小) を選択します。

[Full Screen Mode] (全画面モード)

全画面モードに切り替えると、ターゲットの全画面が表示され、ターゲット サーバと同じ解像度になります。このモードを終了するためのホットキーは、[Options] (オプション) ダイアログ ボックスで指定します。「*ツール オプション* 『*81*p. 』」を参照してください。

全画面モードになっているときに、マウス ポインタを画面上端に移動すると、全画面モード メニュー バーが表示されます。全画面モードの場合でもメニュー バーを表示したままにする場合は、[Tool] (ツール) の [Options] (オプション) ダイアログ ボックスの [Pin Menu Toolbar] (メニュー ツールバーを常に表示] を有効にします。「*ツール オプション* 『*81*p. 』」を参照してください。

▶ 全画面モードに切り替えるには、以下の手順に従います。

- [View] (表示) の [Full Screen] (全画面) を選択します。

▶ 全画面モードを終了するには、以下の手順に従います。

- [Tool] (ツール) の [Options] (オプション) ダイアログで設定されているホットキーを押します。デフォルトは Ctrl+Alt+M です。

常に全画面モードの状態でターゲットにアクセスしたい場合、全画面モードをデフォルトにすることができます。

▶ 全画面モードをデフォルトに設定するには

1. [Tools] (ツール) メニューの [Options] (オプション) をクリックし、[Options] (オプション) ダイアログ ボックスを開きます。
2. [Enable Launch in Full Screen Mode] (全画面モードで起動する) を選択し、[OK] (OK) をクリックします。

ヘルプのオプション

[About Raritan Virtual KVM Client] (バージョン情報)

このメニュー コマンドを選択すると、Virtual KVM Client のバージョン情報が表示されます。このバージョン情報は、ラリタン テクニカル サポートを利用するときに必要になります。

▶ バージョン情報を調べるには、以下の手順に従います。

1. [Help] (ヘルプ) の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。
2. 後でサポート時にアクセスできるように、[Copy to Clipboard] (クリップボードにコピー) ボタンを使用して、ダイアログ ボックスに含まれている情報をクリップボード ファイルにコピーします (必要な場合)。

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) は、Raritan 製品ラインに対応するグラフィカル ユーザ インタフェースです。Raritan KVM over IP デバイスに接続されているターゲット サーバへのリモート アクセスを提供します。MPC の使用方法については、Raritan の Web サイトでユーザ ガイドと同じページから入手できる『KVM and Serial Access Client Guide』を参照してください。MPC の起動手順が記載されています。

このクライアントは Raritan の各種製品で使用されていることに注意してください。このように、ヘルプのこのセクションには、他の製品への参照が表示される場合があります。

Web ブラウザからの MPC の起動

重要: ブラウザの種類を問わず、MPC を開くためには、Dominion デバイスの IP アドレスからのポップアップを許可する必要があります。

重要: Intel® プロセッサを搭載した Mac OS X 10.5/10.6 コンピュータは JRE 1.6 を実行できるので、クライアントとして使用できます。Mac OS X 10.5.8 は、スタンドアロン クライアントとして MPC をサポートしていません。

1. サポートされるブラウザを実行しているクライアントから MPC を開くには、アドレス フィールドに「http://IP-ADDRESS/mpc」と入力します (IP-ADDRESS はラリタン デバイスの IP アドレスに置き換えてください)。MPC が新しいウィンドウに開かれます。

   注: Alt+Tab コマンドで、ローカル システム上のウィンドウ間のみでの切り替えができます。

   MPC が開かれると、自動的に検出されたラリタン デバイスおよびサブネット上で見つかったラリタン デバイスがナビゲータにツリー形式で表示されます。
2. 使用しているデバイスの名前がナビゲータに表示されていない場合は、以下の手順に従って手動で追加します。
   a. [Connection] (接続)、[New Profile] (新しいプロファイル) の順に選択します。[Add Connection] (接続の追加) ウィンドウが開きます。
   b. [Add Connection] (接続の追加) ウィンドウで、デバイスの説明を入力し、接続タイプを指定し、デバイスの IP アドレスを追加して、[OK] をクリックします。この指定内容は後で編集できます。
3. 画面左のナビゲータ パネルで、接続するラリタン デバイスに対応するアイコンをダブルクリックします。

注: お使いのブラウザおよびブラウザのセキュリティ設定によっては、さまざまなセキュリティや証明書に関する確認メッセージまたは警告メッセージが表示されることがあります。MPC を開くには、オプションを承諾する必要があります。

注: Firefox 3.0.3 を使用している場合は、アプリケーションの起動で問題が発生することがあります。この場合は、ブラウザのキャッシュをクリアして、アプリケーションを再起動してください。

Ch 4 仮想メディア

この章の内容

概要

KVM の機能を拡張する仮想メディアを使うことで、クライアント PC やネットワーク ファイル サーバ上のメディアに、リモートの KVM ターゲット サーバからアクセスできるようになります。LX では、ハード ディスク ドライブとリモートでマウントされたイメージの仮想メディア アクセスをサポートします。

D2CIM-VUSB CIM および D2CIM-DVUSB CIM（コンピュータ インタフェース モジュール）では、USB 2.0 インタフェースをサポートする KVM ターゲット サーバへの仮想メディア セッションがサポートされます。これらの CIM では、ずれないマウス機能やリモート ファームウェア アップデートもサポートされます。

仮想メディアを使用することで、以下のような作業をリモートから実行できるようになります。

- ファイルの転送
- 診断の実行
- アプリケーションのインストールと修正パッチ（patch）の適用
- オペレーティング システムの完全インストール

Windows®、Mac®、Linux™ の各クライアントでは、以下の仮想メディア タイプがサポートされています。

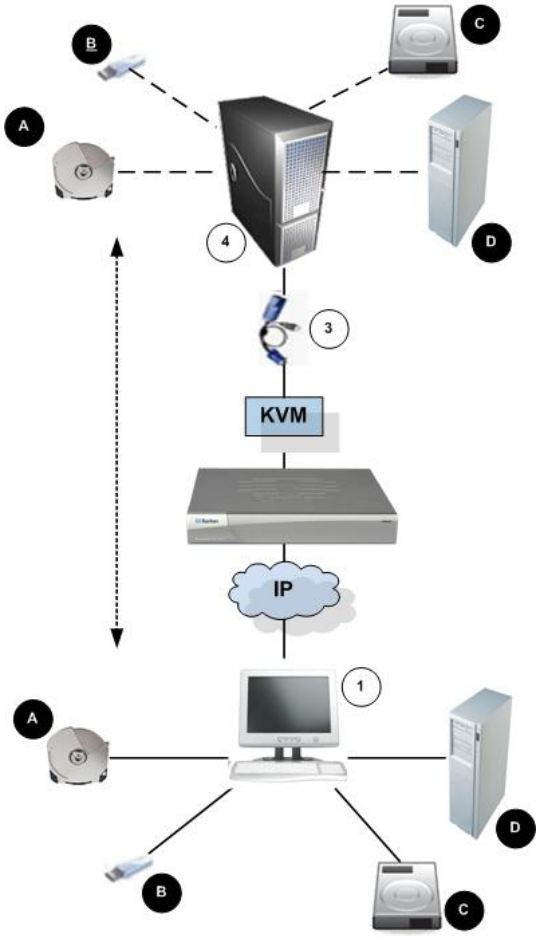
- 内蔵または USB マウントされた CD ドライブや DVD ドライブ
- USB マス ストレージ デバイス
- PC ハード ディスク ドライブ
- ISO イメージ（ディスク イメージ）

注: ラリタンは ISO9660 を標準でサポートしています。ただし、他の ISO 標準も使用できます。

サポートされているクライアント オペレーティング システムは次のとおりです。

- Windows
- Mac OS X 10.5
- Mac OS X 10.6
- Red Hat Desktop 4.0 および 5.0
- openSUSE 10、11
- Fedora 13 および 14

仮想メディア タイプのマウントには、Virtual KVM Client（VKC）および Multi-Platform Client（MPC）を使用できます。ただし、Mac OS X 10.5 の場合は、MPC だけを使用できます。



図の説明			
1	デスクトップ PC	A	CD/DVD ドライブ
2	LX	B	USB マス ストレージ デバイス
3	CIM	C	PC ハード ディスク ドライブ
4	ターゲット サーバ	D	リモート ファイル サーバ (ISO イメージ)

仮想メディアを使用するための条件

仮想メディア機能では、現在ターゲットに適用されている USB プロファイルがサポートする最大 2 台のドライブ（異なるタイプ）をマウントできます。このドライブは、KVM セッションの間のみアクセスできます。

たとえば、特定の CD-ROM をマウントして、それを使用し、作業が終了したらアンマウントすることができます。それでも、別の CD-ROM を仮想的にマウントできるように、この CD-ROM 仮想メディアの "チャンネル" は開いたままになります。こうした仮想メディアの "チャンネル" は、USB プロファイルでサポートされている限り、KVM セッションが閉じられるまで開いたままになります。

仮想メディアを使用するには、ターゲット サーバからアクセスするメディアをクライアントまたはネットワーク ファイル サーバに接続します。この手順を最初に行う必要はありませんが、このメディアへのアクセスを試行する前に行う必要があります。

仮想メディアを使用するには、次の条件が満たされている必要があります。**a**

Dominion デバイス

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス（VM アクセス ポート権限）を許可するようにデバイスを設定する必要があります。ポート権限はグループレベルで設定されます。
- デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- PC 共有を使用する場合は、[Security Settings]（セキュリティ設定）ページでセキュリティ設定を有効にする必要があります。**（オプション）**
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。

クライアント PC

- 仮想メディアの一部のオプションを使用するには、クライアント PC に対する管理者特権が必要です（ドライブ全体のドライブ リダイレクト機能など）。

注:Microsoft Vista または Windows 7 を使用している場合は、ユーザー アカウント制御を無効にするか、Internet Explorer を起動するときに［管理者として実行］を選択します。このためには、［スタート］メニューの［Internet Explorer］を右クリックし、［管理者として実行］を選択します。

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- Windows 2000 が動作する KVM ターゲット サーバには、最新の修正プログラムがすべてインストールされている必要があります。
- USB 2.0 の方が高速なため、推奨されます。

Linux 環境での仮想メディア

以下は、Linux® ユーザ向けの仮想メディアの使用に関する重要情報です。

root ユーザ権限の要件

- Linux クライアントからターゲットに CD ROM をマウントし、その後 CD ROM のマウントを解除する場合は、仮想メディア接続が切断されることがあります。フロッピー ドライブをマウントし、その後フロッピー ディスクを削除した場合も、接続が切断されます。この問題を回避するには、root ユーザであることが必要です。

権限

ドライブ/CD-ROM をターゲットに接続するためには、ユーザが適切なアクセス権限を持っている必要があります。そのためには、以下を使用してチェックします。

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

上の例で、権限は読み取りアクセスの許可に変更されます。

ファイル ユーティリティで ACL をサポートしているシステムでは、ls コマンドの動作は次のように変わります。

- デフォルト ACL または 4 つ以上の必須 ACL エントリを含むアクセス ACL を持つファイルの場合、ls –l で出力される long 形式の ls(1) ユーティリティでは、権限文字列の後に常にプラス記号（+）が表示されます。

これは、/dev/sr0 を使用した例で示されています。getfacl -a /dev/sr0 を使用して、ユーザが ACL に含まれるアクセスを付与されているかどうかを表示しています。この場合は、アクセスが付与されているので、cd-rom をターゲットに接続できます。これは、ls -l コマンドの出力ではそれ以外を示していても関係ありません。

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl:Removing leading '/' from absolute path names
# file:dev/sr0
# owner:root
# group:cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

リムーバブル デバイスの同様の権限チェックを示します。

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;  getfacl -a /dev/sdb1
getfacl:Removing leading '/' from absolute path names
# file:dev/sdb1
# owner:root
# group:disk
user::rw-
group::rw-
other::---
```

これは、ユーザにそのリムーバブル デバイスの読み取り専用許可が付与されていることを要求します。

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

これで、ドライブをターゲットに接続できるようになります。

読み取り/書き込み可能に設定できない状況

以下の場合、仮想メディアを読み取り/書き込み可能にすることはできません。

- Linux® および Mac® の各クライアント
- 複数のハード ディスク ドライブすべてが対象の場合
- ドライブが書き込み保護されている場合
- ユーザに読み取り/書き込みの権限がない場合。
  - ポート権限の [Access] (アクセス) が [None] (なし) または [View] (表示) に設定されている場合。
  - ポート権限の [VM Access] (VM アクセス) が [Read-Only] (読み取り専用) または [Deny] (拒否) に設定されている場合。

仮想メディアの使用

仮想メディアの使用を開始する前に「*仮想メディアを使用するための前提条件* 『*93*p. の"*仮想メディアを使用するための条件*"参照 』」を参照してください。

▶ 仮想メディアを使用するには、以下の手順に従います。

1. ファイル サーバ ISO イメージにアクセスする場合は、リモート コンソールの［ファイル サーバのセットアップ］ページを使用して、ファイル サーバとイメージを指定してください。「*仮想メディア ファイル サーバのセットアップ（ファイル サーバ ISO イメージの場合のみ）* 『*98*p. 』」を参照してください。

   注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

2. 適切なターゲット サーバとの KVM セッションを開きます。
   a. リモート コンソールで［ポート アクセス］ページを開きます。
   b. ［ポート アクセス］ページでターゲット サーバに接続します。
   - 適切なサーバのポート名をクリックします。
   - ［ポート アクション］メニューの［接続］コマンドを選択します。Virtual KVM Client ウィンドウにターゲット サーバが表示されます。

3. 仮想メディアに接続します。

対象メディア	選択する VM オプション
ローカル ドライブ	［ドライブの接続］
ローカル CD/DVD ドライブ	［CD-ROM/ISO の接続］
ISO イメージ	［CD-ROM/ISO の接続］
ファイル サーバ ISO イメージ	［CD-ROM/ISO の接続］

作業が終わったら、仮想メディアを切断します。「*仮想メディアの切断* 『*103*p. 』」を参照してください。

仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)

注: この機能は、仮想メディアを使用してファイル サーバ ISO イメージにアクセスする場合にのみ必要です。Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

注: ファイル サーバには、SMB/CIFS のサポートが必要です。

リモート コンソールの [File Server Setup] (ファイル サーバのセットアップ) ページで、仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指定します。ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image] (リモート サーバの ISO イメージ) で [Hostname] (ホスト名) および [Image] (イメージ) ドロップダウンリスト ([Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックス) の選択肢として表示されます。「*CD-ROM/DVD-ROM/ISO イメージのマウント* 『*101*p. 』」を参照してください。

▶ 仮想メディアとしてアクセスするファイル サーバ ISO イメージを指定するには、以下の手順に従います。

1. リモート コンソールから仮想メディアを選択します。[File Server Setup] (ファイル サーバのセットアップ) ページが開きます。
2. 仮想メディアとしてアクセスするすべてのメディアについて、[Selected] (選択) チェックボックスをオンにします。
3. アクセスするファイル サーバ ISO イメージに関する情報を入力します。
   - [IP Address/Host Name] (IP アドレス/ホスト名) - ファイル サーバのホスト名または IP アドレスです。
   - [Image Path] (イメージのパス) - ISO イメージの場所を表す完全パス名です。たとえば、/sharename0/path0/image0.iso、¥sharename1¥path1¥image1.iso などです。

   注: ホスト名は 232 文字以内で指定してください。
4. [Save] (保存) をクリックします。これで、指定したすべてのメディアが [Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスで選択できるようになりました。

注: LX、KX、KSX、または KX101 G2 デバイスで使用されるサードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

注:Windows 2003® サーバに接続してサーバから ISO イメージをロードしようとしている場合は、「Virtual Media mounting on port failed. (ポート上でマウントしている仮想メディアに障害が発生しました。)Unable to connect to the file server or incorrect File Server username and password (ファイル サーバに接続できないか、ファイル サーバのユーザ名またはパスワードが正しくありません)」というエラーが発生することがあります。このエラーが発生する場合は、[Microsoft Network Server: Digitally Sign Communications] (Microsoft ネットワーク サーバ: デジタル的に、通信にデジタル署名を行う) を無効にします。

注: Windows 2003 Server に接続し、サーバから ISO イメージをロードしようとすると、「Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password」(ポートで仮想メディアのマウントに失敗しました。ファイル サーバに接続できないか、ファイル サーバのユーザ名とパスワードが正しくありません) というエラーが表示される場合があります。このエラーが発生した場合は、ドメイン コントローラ ポリシーでサーバの [Microsoft ネットワーク サーバー: 通信にデジタル署名を行う] オプションを無効にします。

仮想メディアへの接続

ローカル ドライブのマウント

このオプションを使用すると、ドライブ全体がマウントされます。つまり、クライアントコンピュータのディスク ドライブ全体がターゲット サーバに仮想的にマウントされます。このオプションは、ハード ディスク ドライブと外部ドライブにのみ使用してください。ネットワーク ドライブ、CD-ROM ドライブ、または DVD-ROM ドライブは対象外です。これは、[Read/Write](読み取り/書き込み可能) を指定できる唯一のオプションです。

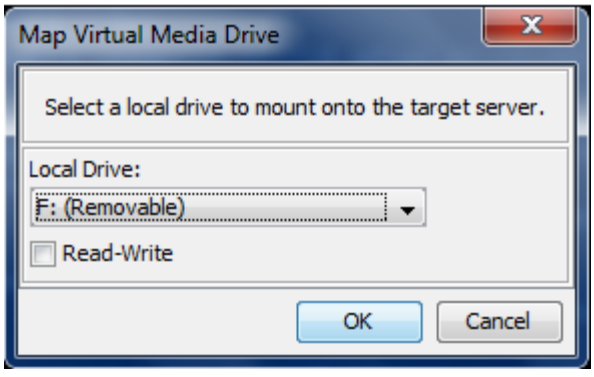
注: 特定のバージョンの Windows オペレーティング システムが動作している KVM ターゲット サーバでは、NTFS 形式のパーティション (ローカル C ドライブなど) がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合があります。

その場合には、リモート コンソールを閉じて再接続した後で、別の仮想メディア デバイスをリダイレクトしてください。同じターゲット サーバに別のユーザーが接続している場合、そのユーザーの接続も閉じる必要があります。

注: KX II 2.1.0 以降では、フロッピー ディスクなどの外部ドライブをマウントすると、ドライブの LED ライトが点灯したままになります。これは、デバイスが 500 ミリ秒ごとにドライブをチェックして、ドライブがまだマウントされているかどうかを確認するからです。

▶ **クライアント コンピュータのドライブにアクセスするには、以下の手順に従います。**

1. Virtual KVM Client で、[Virtual Media](仮想メディア) の [Connect Drive](ドライブの接続) を選択します。[Map Virtual Media Drive](仮想メディア ドライブの割り当て) ダイアログ ボックスが表示されます。()



2. [Local Drive](ローカル ドライブ) ドロップダウン リストから、ドライブを選択します。

3. 読み取りと書き込みの機能が必要な場合には、[Read-Write] (読み取り/書き込み可能) チェックボックスをオンにします。このオプションは、リムーバブル ドライブ以外では無効になっています。詳細は、「*読み取り/書き込み可能に設定できない状況 『96*p. 』」を参照してください。このチェックボックスをオンにすると、接続した USB ディスクに読み取りと書き込みを実行できるようになります。

警告: 読み取り/書き込みアクセスを有効にすると危険な場合があります。同じドライブに対して同時に複数のクライアント PC からアクセスすると、データが壊れる恐れがあります。書き込みアクセスが不要な場合は、このオプションをオフのままにしてください。

4. [接続] をクリックします。メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

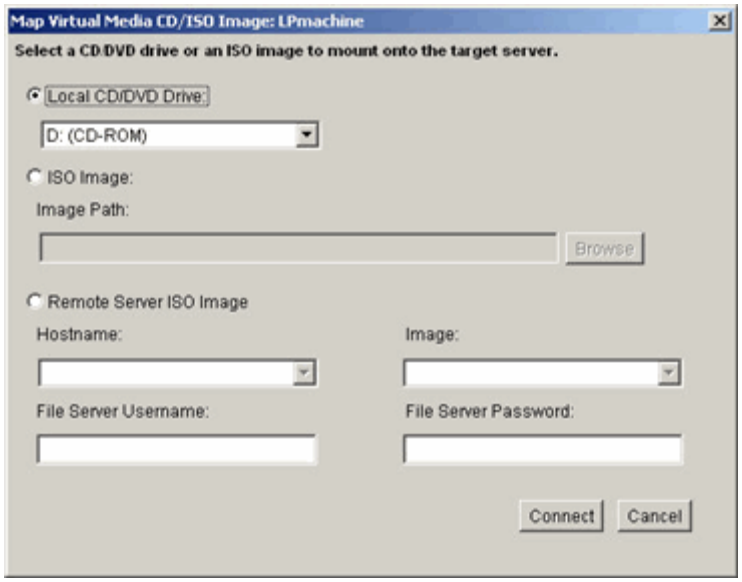
CD-ROM/DVD-ROM/ISO イメージのマウント

このオプションを使用して、CD-ROM、DVD-ROM、ISO イメージをマウントします。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

▶ **CD-ROM、DVD-ROM、ISO イメージにアクセスするには、以下の手順に従います。**

1. Virtual KVM Client で、[仮想メディア] の [CD-ROM/ISO イメージに接続] を選択します。[仮想メディア CD/ISO イメージの割り当て] ダイアログ ボックスが表示されます。



2. 内部および外部の CD-ROM ドライブまたは DVD-ROM ドライブの場合
   a. ［ローカル CD/DVD ドライブ］を選択します。
   b. ［ローカル CD/DVD ドライブ］ドロップダウン リストから、ドライブを選択します。使用可能なすべての内部/外部の CD ドライブおよび DVD ドライブの名前が、ドロップダウン リストに表示されます。
   c. ［接続］をクリックします。
3. ISO イメージの場合
   a. ［ISO イメージ］オプションを選択します。CD、DVD、またはハード ディスクのディスク イメージにアクセスする場合に、このオプションを使用します。サポートされる形式は ISO 形式のみです。
   b. ［参照］をクリックします。
   c. 使用するディスク イメージが含まれるパスを指定して、［開く］をクリックします。パスが［イメージのパス］フィールドに入力されます。
   d. ［接続］をクリックします。
4. ファイル サーバ上のリモート ISO イメージの場合
   a. ［リモート サーバの ISO イメージ］オプションを選択します。
   b. ドロップダウン リストから、ホスト名とイメージを選択します。ファイル サーバとイメージ パスは、［ファイル サーバのセットアップ］ページを使用して設定できます。［ファイル サーバのセットアップ］ページで設定した項目がドロップダウン リストに表示されます。
   c. ［ファイル サーバ ユーザ名］: ファイル サーバへのアクセスに必要なユーザ名です。名前には、mydomain/username のようにドメイン名を含めることができます。
   d. ［ファイル サーバ パスワード］: ファイル サーバへのアクセスに必要なパスワードです（入力時、フィールドはマスクされます）。
   e. ［接続］をクリックします。

メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

注: Linux® ターゲット上のファイルを操作する場合、仮想メディアを使用してコピーしたファイルを表示するには、コピー後に Linux の Sync コマンドを使用します。Sync コマンドを実行するまではファイルを表示できません。

注: Windows 7® オペレーティング システム® を使用している場合、デフォルトでは、ローカル CD/DVD ドライブまたはリモート ISO イメージをマウントしたとき、リムーバブル ディスクは Windows の［マイ コンピュータ］フォルダに表示されません。ローカル CD/DVD ドライブまたはリモート ISO イメージをこのフォルダに表示するには、［ツール］メニューの［フォルダ オプション］をクリックし、［空のドライブは［コンピュータ］フォルダに表示しない］チェック ボックスをオフにします。

注: サードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

仮想メディアの切断

▶ **仮想メディア ドライブを切断するには、以下の手順に従います。**

- ローカル ドライブの場合は、[Virtual Media]（仮想メディア）の [Disconnect Drive]（ドライブの切断）を選択します。
- CD-ROM、DVD-ROM、ISO イメージの場合は、[Virtual Media]（仮想メディア）の [Disconnect CD-ROM/ISO Image]（CD-ROM/ISO イメージの切断）を選択します。

注: 切断コマンドを使用する方法だけでなく、KVM 接続を閉じても仮想メディアが切断されます。

Ch 5 [User Management] (ユーザ管理)

この章の内容

ユーザ グループ

LX は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内部リストを保持しています。この情報は、暗号化形式で内部に保存されます。認証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。すべてのユーザは認証を受ける必要があります。LDAP/LDAPS または RADIUS 認証を行うように LX が設定されている場合、その認証が行われた後に、ローカル認証が行われます。

すべての LX には、3 つのデフォルト ユーザ グループが存在します。これらのグループは削除できません。

ユーザ	説明
Admin (管理者)	このグループに所属するユーザは、完全な管理者特権を持ちます。元の製品出荷時のデフォルト ユーザはこのグループのメンバーであり、完全なシステム特権を持ちます。さらに、Admin (管理者) ユーザは Admin (管理者) グループのメンバーである必要があります。
Unknown (不明)	LDAP/LDAPS または RADIUS を使用して外部的に認証されるユーザまたはシステムで既知のユーザのデフォルト グループです。外部 LDAP/LDAPS サーバまたは RADIUS サーバによって有効なユーザ グループが識別されなかった場合、Unknown (不明) グループが使用されます。さらに、新規に作成されたユーザは別のグループに割り当てられるまでこのグループに自動的に配置されます。
Individual Group (個別グループ)	個別グループとは、基本的に個人の「グループ」です。つまり、特定のユーザは独自のグループに属し、他の実際のグループには属しません。個別グループは、グループ名の先頭に "@" が付けられているので区別できます。個別グループでは、グループと同じ権限をユーザ アカウントに割り当てることができます。

LX 内では最大 254 個のユーザ グループを作成できます。 LX 内では最大 254 個のユーザ グループを作成できます。

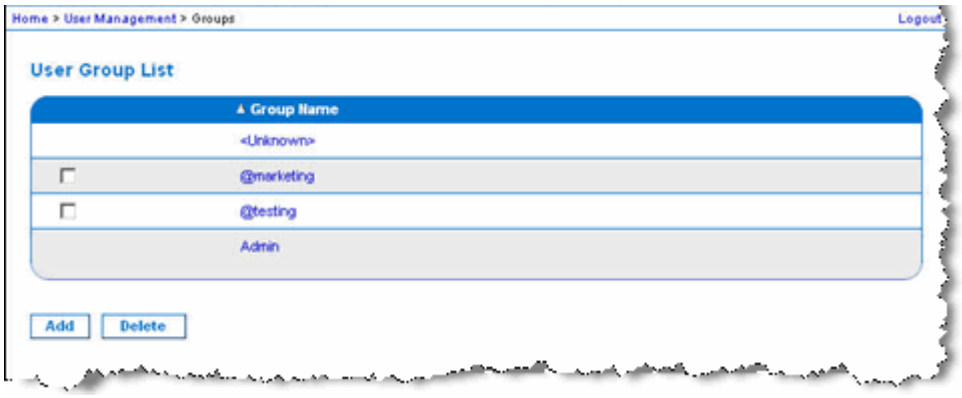
ユーザ グループ リスト

ユーザ グループは、ローカル認証とリモート認証 (RADIUS または LDAP/LDAPS) で使用されます。個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

[ユーザ グループ リスト] ページには、すべてのユーザ グループのリストが表示されます。このリストは、[グループ名] 列見出しをクリックすることで、昇順または降順に並べ替えることができます。[ユーザ グループ リスト] ページでは、ユーザ グループを追加、変更、または削除することもできます。

▶ **ユーザ グループのリストを表示するには、以下の手順に従います。**

- [ユーザ管理] の [ユーザ グループ リスト] を選択します。[ユーザ グループ リスト] ページが開きます。



ユーザとグループの関係

ユーザはグループに属し、グループには特権が割り当てられています。LX の各種のユーザをグループに分けることにより、ユーザごとに許可を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能です。その場合は、ユーザを「個別」として分類します。

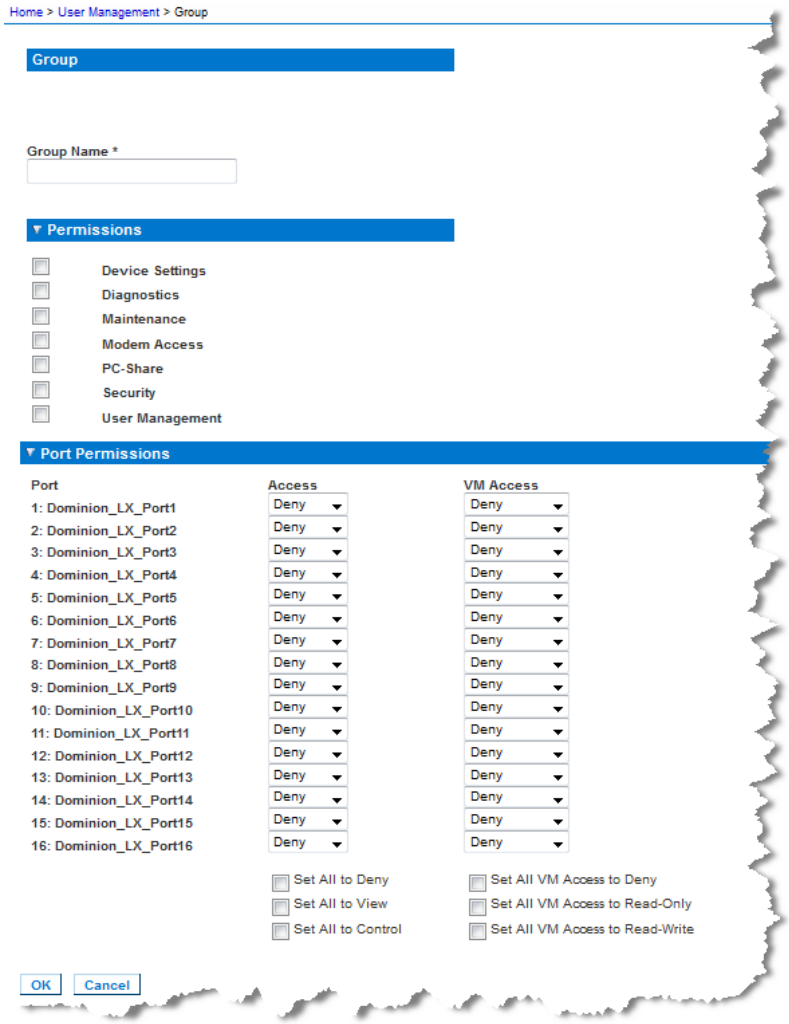
認証が成功すると、デバイスは、グループ情報を使用して、アクセスできるサーバ ポート、デバイスの再起動を許可するかどうかなど、そのユーザの許可を決定します。

新規ユーザ グループの追加

▶ **新規ユーザ グループを追加するには、以下の手順に従います。**

1. [ユーザ管理] の [新規ユーザ グループの追加] を選択するか、[ユーザ グループ リスト] ページの [追加] をクリックします。
2. [グループ名] フィールドに、新しいユーザ グループのわかりやすい名前 (最大 64 文字) を入力します。
3. このグループに属するすべてのユーザに対して割り当てる許可の横にあるチェックボックスをオンにします。「*許可の設定* 『*107*p. 』」を参照してください。
4. [OK] (OK) をクリックします。

注: 複数の管理機能を MPC 内および LX ローカル コンソールから利用できます。これらの機能を利用できるのは、デフォルトの Admin (管理者) グループのメンバーに限られます。



許可の設定

重要: [ユーザ管理] チェックボックスをオンにすると、グループのメンバーは、自身も含むすべてのユーザの許可を変更することができます。これらの許可を付与する場合は注意してください。

許可	説明
[デバイス設定]	ネットワーク設定、日付/時刻設定、ポート設定 (チャンネル名など)、イベント管理 (SNMP、Syslog)、仮想メディア ファイル サーバのセッ

許可	説明
	トアップ。
[診断]	ネットワーク インタフェース ステータス、ネットワーク統計、ホストへの Ping、ホストへのトレース ルート、LX 診断
[保守]	データベースのバックアップと復元、ファームウェアのアップグレード、ファクトリ リセット、再起動
[モデム アクセス]	モデムを使用して LX デバイスに接続する許可。
[PC 共有]	複数のユーザによる同一ターゲットへの同時アクセス カスケード接続構成にしており、ベース LX デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合、すべてのデバイス間で同じ PC 共有設定を共有する必要があります。カスケード接続の詳細については、「***カスケード接続の設定および有効化*** ***『135p. 』***」を参照してください。
[セキュリティ]	SSL 証明書、セキュリティ設定 (VM 共有、PC 共有)
[ユーザ管理]	ユーザおよびグループの管理、リモート、認証 (LDAP/LDAPS/RADIUS)、ログイン設定 カスケード接続構成にしており、ベース LX デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合、ユーザ設定、ユーザ グループ設定、およびリモート認証設定をすべてのデバイス間で統一する必要があります。カスケード接続の詳細については、「***カスケード接続の設定および有効化*** ***『135p. 』***」を参照してください。

ポート権限の設定

それぞれのサーバ ポートに対して、そのグループが持つアクセスのタイプ、および仮想メディアへのポート アクセスのタイプを指定できます。すべての権限についてデフォルト設定はすべて［拒否］になっていることに注意してください。

ポート アクセス

オプション	説明
［拒否］	アクセスを完全に拒否します。
［表示］	ビデオを表示しますが、接続先のターゲット サーバの操作はできません。
［制御］	接続先のターゲット サーバを制御します。VM の場合は、グループに［制御］を割り当てる必要があります。 追加された KVM スイッチをユーザ グループ内のすべてのユーザが表示できるようにするためには、各ユーザに［制御］アクセスが付与されている必要があります。この権限を持たないユーザには、KVM スイッチが後で追加されても、スイッチは表示されません。

VM アクセス

オプション	説明
［拒否］	ポートに対して仮想メディア許可はすべて拒否されます。
［読み取り専用］	仮想メディア アクセスは、読み取りアクセスのみに制限されます。
［読み取り/書き込み可能］	仮想メディアに対する完全なアクセス（読み取り、書き込み）が許可されます。

ティアー接続構成にしており、ベース LX デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、カスケード接続デバイスでは個別のポート制御レベルが適用されます。カスケード接続の詳細については、「*カスケード接続の設定および有効化 『135*p. *』*」を参照してください。

個別グループの許可の設定

▶ 個別ユーザ グループに許可を設定するには、以下の手順に従います。

1. グループ リストから目的のグループを探します。個別グループは、グループ名の先頭に @ が付けられているので区別できます。
2. グループ名をクリックします。[Group](グループ) ページが開きます。
3. 適切な許可を選択します。
4. [OK] をクリックします。

既存のユーザ グループの変更

注: Admin (管理者) グループに対しては、すべての許可が有効になっています。この設定は変更できません。

▶ 既存のユーザ グループを変更するには、以下の手順に従います。

1. [グループ] ページで、適切なフィールドを変更し、適切な許可を設定します。
2. グループに対する許可を設定します。このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。「*許可の設定* 『*107*p. 』」を参照してください。
3. [ポート権限] を設定します。このグループに属するユーザがアクセスできるサーバ ポート (およびアクセスのタイプ) を指定します。「*ポート権限の設定* 『*109*p. 』」を参照してください。
4. [OK] をクリックします。

▶ ユーザ グループを削除するには、以下の手順に従います。

重要: ユーザを含むグループを削除すると、そのユーザは <不明> ユーザ グループに自動的に割り当てられます。

ヒント: 特定のグループに属しているユーザを調べるには、ユーザ グループ別にユーザ リストを並べ替えます。

1. リストのグループ名の左にあるチェックボックスをオンにして、目的のグループを選択します。
2. [削除] をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

ユーザ

ユーザが LX にアクセスするには、ユーザ名とパスワードを付与されている必要があります。この情報は、LX にアクセスしようとしているユーザを認証するために使用されます。 各ユーザ グループに対して最大 254 個のユーザを作成できます。

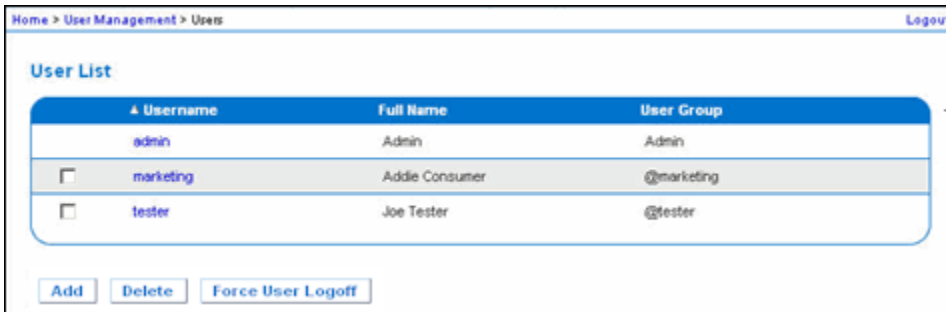
ティアー接続構成にしており、ベース LX デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ユーザは、ベース デバイスにアクセスする許可、および、(必要に応じて) 個々のティアー接続デバイスにアクセスする許可を必要とします。ユーザがベース デバイスにログオンすると、各ティアー接続デバイスが照会され、ユーザは、アクセス許可を得ている各ターゲット サーバにアクセスできます。 ティアー接続の詳細については、「*ティアー接続を設定および有効化する『135*p. の*″カスケード接続の設定および有効化″*参照 』」を参照してください。

[User List] (ユーザ リスト)

[User List] (ユーザ リスト) ページには、すべてのユーザについて、ユーザ名、フル ネーム、およびユーザ グループが表示されます。このリストは、任意の列名をクリックすることで並べ替えることができます。[User List] (ユーザ リスト) ページでは、ユーザを追加、変更、または削除することもできます。

▶ ユーザ リストを表示するには、以下の手順に従います。

- [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択します。[User List] (ユーザ リスト) ページが開きます。



新規ユーザの追加

LX ユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。「**新規ユーザ グループの追加『106p. 』**」を参照してください。

[User] (ユーザ) ページでは、新規ユーザの追加、ユーザ情報の変更、無効化されているユーザの再有効化を行うことができます。

注: ユーザがログインに失敗した回数が [Security Settings] (セキュリティ設定) ページで設定されているログイン失敗の最大許容回数を超えた場合、そのユーザ名は無効化されます。「セキュリティの設定」を参照してください。

▶ 新規ユーザを追加するには、以下の手順に従います。

1. [ユーザ管理] の [新規ユーザの追加] を選択するか、[ユーザ リスト] ページの [追加] をクリックします。
2. [ユーザ名] フィールドに、一意のユーザ名を入力します (最大 16 文字)。
3. [フル ネーム] フィールドに、ユーザのフル ネームを入力します (最大 64 文字)。
4. [パスワード] フィールドにパスワードを入力し、[パスワードの確認] フィールドにパスワードを再入力します (最大 64 文字)。
5. [ユーザ グループ] ドロップダウン リストからグループを選択します。

   このユーザを既存のユーザ グループに関連付けたくない場合は、ドロップダウン リストから [Individual Group] (個別グループ) を選択します。個別グループの許可についての詳細は、「***個別グループの許可の設定 『110p. 』***」を参照してください。
6. 新規ユーザを有効にするには、[アクティブ] チェックボックスをオンのままにします。[OK] をクリックします。

既存のユーザ グループの変更

▶ 既存のユーザを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択して、[User List] (ユーザ リスト) ページを開きます。
2. [User List] (ユーザ リスト) ページのリストから目的のユーザを探します。
3. ユーザ名をクリックします。[User] (ユーザ) ページが開きます。

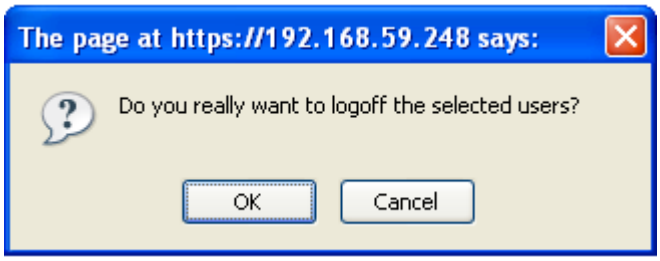
4. [User] (ユーザ) ページで、目的のフィールドを変更します [User] (ユーザ) ページにアクセスする方法についての詳細は、「*新規ユーザの追加* 『*112*p. 』」を参照してください。
5. ユーザを削除するには、[Delete] (削除) をクリックします。削除してよいかどうかを確認するダイアログ ボックスが開きます。
6. [OK] (OK) をクリックします。

ユーザのログオフ (強制ログオフ)

管理者である場合は、LX にログオンしている他のユーザのうち、ローカルに認証されているユーザをログオフすることができます。

▶ **ユーザをログオフするには、以下の手順に従います。**

1. [ユーザ管理] の [ユーザ リスト] を選択して [ユーザ リスト] ページを開くか、ページの左側のパネルの [接続中のユーザ] リンクをクリックします。
2. [ユーザ リスト] ページのリストから目的のユーザを探し、その名前の横のチェックボックスをオンにします。
3. [ユーザの強制ログオフ] をクリックします。
4. [ユーザのログオフ] ダイアログ ボックスで [OK] をクリックして、そのユーザを強制的にログオフします。



5. ユーザがログオフしたことを示す確認メッセージが表示されます。このメッセージには、ログオフした日時が表示されます。[OK] をクリックして、メッセージを閉じます。

[Authentication Settings] (認証設定)

認証とは、ユーザが本物であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

LX がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

ティアー接続構成にしており、ベース LX デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ベース デバイスと各ティアー接続デバイスで同じ認証設定を使用する必要があります。

[Authentication Settings] (認証設定) ページでは、LX へのアクセスに使用する認証の種類を設定できます。

注: リモート認証 (LDAP/LDAPS または RADIUS) を選択すると、ユーザが見つからない場合はローカル認証データベースも確認されます。

▶ 認証を設定するには、以下の手順に従います。

1. [ユーザ管理] の [認証設定] を選択します。[認証設定] ページが開きます。
2. 使用する認証プロトコルのオプションを選択します ([ローカル認証]、[LDAP/LDAPS]、または [RADIUS])。[LDAP] オプションを選択した場合、LDAP に関連するフィールドが有効になります。[RADIUS] オプションを選択した場合、RADIUS に関連するフィールドが有効になります。
3. [ローカル認証] を選択した場合は、手順 6 に進みます。
4. [LDAP/LDAPS] を選択した場合は、「LDAP/LDAPS リモート認証の実装」を参考にして、[認証設定] ページの [LDAP] セクションの各フィールドを指定してください。
5. [RADIUS] を選択した場合は、「RADIUS リモート認証の実装」を参考にして、[認証設定] ページの [RADIUS] セクションの各フィールドを指定してください。
6. [OK] をクリックして保存します。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [デフォルトに戻す] をクリックします。

LDAP/LDAPS リモート認証の実装

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクトリ サービスを照会および変更するためのネットワーキング プロトコルです。クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアントは、オペレーション要求をサーバに送信します。サーバは、この要求に対して応答を返します。

メモ: Microsoft Active Directory は、LDAP/LDAPS 認証サーバとしてネイティブに機能します。

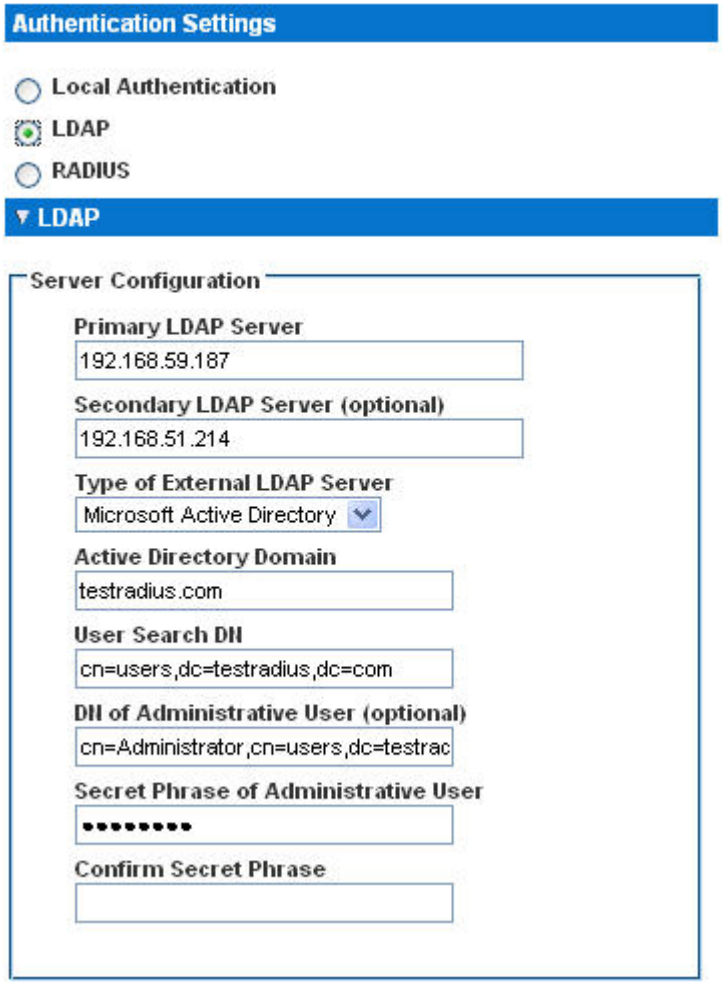
▶ **LDAP 認証プロトコルを使用するには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [LDAP] (LDAP) ラジオ ボタンを選択して、ページの [LDAP] (LDAP) セクションを有効にします。
3. ▶ LDAP アイコンをクリックして、ページの [LDAP] (LDAP) セクションを展開します。

   サーバの設定
4. [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP/LDAPS リモート認証サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにし、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。
5. [Secondary LDAP Server] (セカンダリ LDAP サーバ) フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) オプションをオンにした場合は、DNS 名を使用する必要があります。残りのフィールドについては、[Primary LDAP Server] (プライマリ LDAP サーバ) フィールドの場合と同じ設定を使用します。**(オプション)**
6. [Type of External LDAP Server] (外部 LDAP サーバの種類)。
7. 外部 LDAP/LDAPS サーバを選択します。使用可能なオプションを選択します。
   - [Generic LDAP Server] (一般的な LDAP サーバ)。
   - [Microsoft Active Directory]。Active Directory は、Windows 環境向けの Microsoft による LDAP/LDAPS ディレクトリ サービスの実装です。

8. Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。たとえば、*acme.com* などです。特定のドメインの名前については、Active Directive 管理者にお問い合わせください。
9. [User Search DN] (ユーザ検索 DN) フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。最大 64 文字まで使用できます。たとえば、`cn=Users,dc=raritan,dc=com` というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。
10. [DN of administrative User] (管理者ユーザの DN) フィールドに管理者ユーザの識別名を入力します (最大 64 文字)。このフィールドは、LDAP サーバで管理者に管理者ユーザの役割を使用したユーザ情報の検索を許可している場合にのみ入力します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。たとえば、管理者ユーザの DN として、以下のように設定します。
    `cn=Administrator,cn=Users,dc=testradius,dc=com`**(オプション)**

11. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリモート認証サーバに対して認証するために使用するパスワードを入力する必要があります。[Secret Phrase] (秘密フレーズ) フィールドにパスワードを入力し、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドにパスワードを再入力します (最大 128 文字)。



LDAP/LDAP Secure

12. SSL を使用する場合は、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにします。これにより、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスがオンになります。Secure Sockets Layer (SSL) は、LX が LDAP/LDAPS サーバと安全に通信できるようにする暗号プロトコルです。
13. [Port] (ポート) のデフォルトは 389 です。標準 LDAP TCP ポートを使用するか、または別のポートを指定します。

14. [Secure LDAP Port] (セキュア LDAP ポート) のデフォルトは 636 です。デフォルトのポートを使用するか、または別のポートを指定します。このフィールドは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用します。
15. 前にアップロードしたルート CA 証明書ファイルを使用してサーバから提供された証明書を検証するには、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにします。前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。この機能を無効にすることは、不明な証明機関によって署名された証明書を受け取ることと同じです。このチェックボックスは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用できます。

注: 検証にルート CA 証明書を使用し、さらに [Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにする場合は、サーバ ホスト名がサーバ証明書に記載された共通名と一致する必要があります。

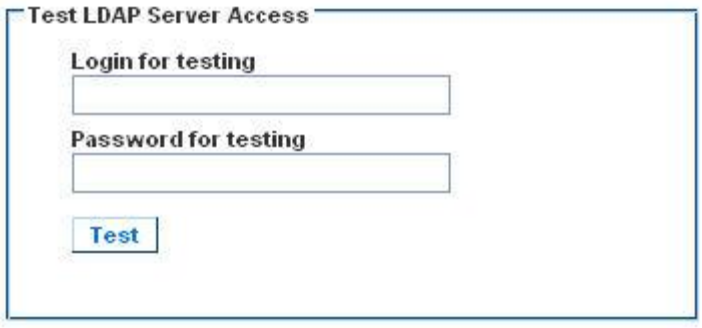
---

16. 必要な場合は、ルート CA 証明書のファイルをアップロードします。このフィールドは、[セキュア LDAP を有効にする] チェックボックスがオンのときに有効になります。LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせてください。[参照] を使用して証明書ファイルを選択します。LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、新しい証明書を有効にするために LX を再起動する必要があります。

LDAP サーバ アクセスのテスト

17. LDAP サーバおよび LX をリモート認証用に正しく構成するために複雑な設定が必要になることがあるので、LX には、[Authentication Settings] (認証設定) ページから LDAP の設定をテストする機能が用意されています。LDAP の設定をテストするには、[Login for testing] (テスト用ログイン) フィールドと [Password for testing] (テスト用パスワード) フィールドにそれぞれログイン名とパスワードを入力します。これは、LX にアクセスするときに入力したユーザ名とパスワードです。LDAP サーバはこれを使用してユーザを認証します。[Test] (テスト) をクリックします。

    テストが完了すると、テストが成功したことを知らせるメッセージが表示されます。テストが失敗した場合は、詳細なエラー メッセージが表示されます。成功したことが表示されるか、または失敗した場合は詳細なエラー メッセージが表示されます。成功時には、リモート LDAP サーバから取得されたテスト ユーザのグループ情報も表示されることがあります。



ユーザ グループ情報を Active Directory サーバから返す

LX では Active Directory® (AD) を使用したユーザ認証がサポートされているので、ユーザを LX でローカルに定義する必要はありません。これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認可と AD ユーザ特権は、標準の LX ポリシー、および AD ユーザ グループにローカルに適用されるユーザ グループ特権によって制御および管理されます。

重要: Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、LX はこの設定をサポートします。この場合、以下に示す手順を実行する必要はありません。AD LDAP/LDAPS スキーマを更新する方法の詳細については、「*LDAP スキーマの更新* 『*218*p. の"*LDAP スキーマを更新する*"参照 』」を参照してください。

▶ LX で AD サーバを有効にするには、以下の手順に従います。

1. LX を使用して、特殊なグループを作成し、適切な許可および特権をグループに割り当てます。たとえば、KVM_Admin や KVM_Operator というグループを作成します。
2. Active Directory サーバで、前の手順で作成したのと同じグループ名を持つ新しいグループを作成します。
3. AD サーバ上で、手順 2 で作成したグループに LX ユーザを割り当てます。
4. LX で、AD サーバを有効にし、適切に設定します。「*LDAP/LDAPS リモート認証の実装* 『*115*p. 』」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- LX には、[管理者] と [<不明>] のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることはできません。Active Directory サーバでこれらと同じグループ名が使用されていないことを確認してください。
- Active Directory サーバから返されたグループ情報が LX のグループ設定と一致しない場合、正常に認証されたユーザに対して自動的に [<不明>] グループが割り当てられます。
- ダイヤルバック番号を使用する場合は、次の文字列を入力する必要があります。大文字と小文字は区別されます。*msRADIUSCallbackNumber*
- Microsoft からの推奨に基づいて、ドメイン ローカル グループではなく、ユーザ アカウントを含むグローバル グループを使用する必要があります。

RADIUS リモート認証の実装

Remote Authentication Dial-in User Service (RADIUS) は、ネットワーク アクセス アプリケーションのための AAA (認証 (authentication)、認可 (authorization)、アカウンティング (accounting)) プロトコルです。

▶ RADIUS 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [RADIUS] (RADIUS) ラジオ ボタンをクリックして、ページの [RADIUS] (RADIUS) セクションを有効にします。
3. ▶ RADIUS アイコンをクリックして、ページの [RADIUS] (RADIUS) セクションを展開します。

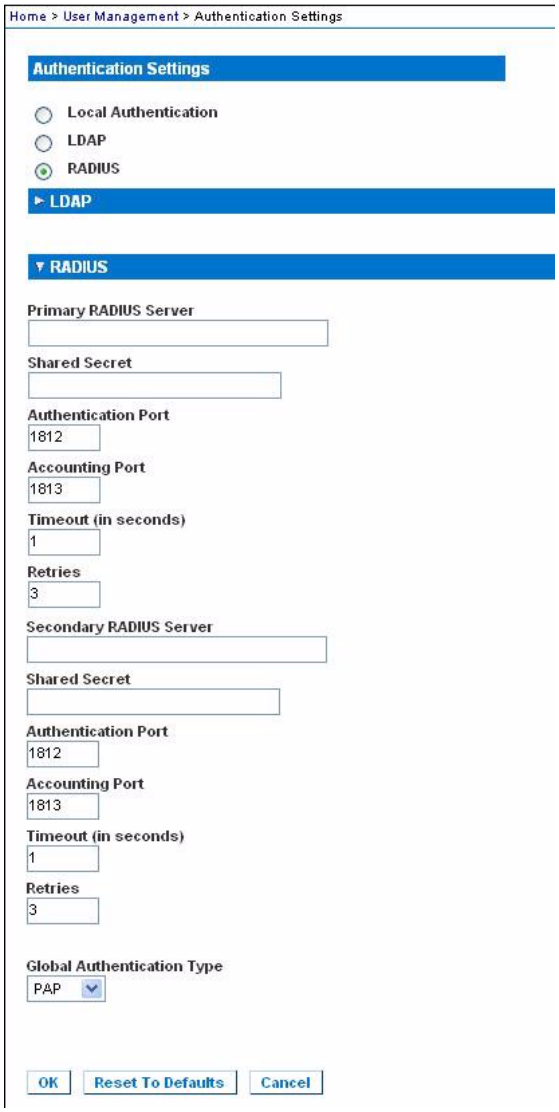
4. [Primary Radius Server] (プライマリ Radius サーバ) フィールドおよび [Secondary Radius Server] (セカンダリ Radius サーバ) フィールドに、プライマリ認証サーバの IP アドレスおよびオプションでセカンダリ認証サーバの IP アドレスを入力します (最大 256 文字)。
5. [Shared Secret] (共有の秘密) フィールドに、認証に使用するサーバの秘密フレーズを入力します (最大 128 文字)。

   共有の秘密とは、LX と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。
6. [Authentication Port] (認証ポート) のデフォルトは 1812 ですが、必要に応じて変更できます。
7. [Accounting Port] (アカウンティング ポート) のデフォルトは 1813 ですが、必要に応じて変更できます。
8. [Timeout] (タイムアウト) は秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。

   このタイムアウトは、LX が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。
9. デフォルトの再試行回数は 3 回です。

   これは、LX が RADIUS サーバに対して認証要求を送信する回数です。
10. ドロップダウン リストのオプションから、適切な [Global Authentication Type] (グローバル認証タイプ) を選択します。
    - [PAP] (PAP) - PAP の場合、パスワードは平文 (ひらぶん) - 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが 1 つのデータ パッケージとして送信されます。

- [CHAP] (CHAP) – CHAP の場合、サーバはいつでも認証を要求できます。CHAP は、PAP よりも高いセキュリティを実現します。



RADIUS 認証用の Cisco ACS 5.x

Cisco ACS 5.x サーバを使用している場合は、LX に RADIUS 認証を設定した後に、Cisco ACS 5.x サーバで以下の手順を完了する必要があります。

注: 以下の手順には、各ページへのアクセスに使用される Cisco のメニューおよびメニュー項目が含まれます。各手順の最新情報とその実行の詳細については、Cisco のマニュアルを参照してください。

- AAA クライアントとしての LX の追加（**必須**）– [Network Resources]（ネットワーク リソース）、[Network Device Group]（ネットワーク デバイス グループ）、[Network Device and AAA Clients]（ネットワーク デバイスと AAA クライアント）の順に選択
- ユーザの追加/編集（**必須**）– [Network Resources]（ネットワーク リソース）、[Users and Identity Stores]（ユーザ ストアと ID ストア）、[Internal Identity Stores]（内部 ID ストア）、[Users]（ユーザ）の順に選択
- CHAP プロトコルを有効にするデフォルト ネットワーク アクセスの設定（**オプション**）– [Policies]（ポリシー）、[Access Services]（アクセス サービス）、[Default Network Access]（デフォルト ネットワーク アクセス）の順に選択
- アクセスを制御する認可ポリシー ルールの作成（**必須**）– [Policy Elements]（ポリシー要素）、[Authorization and Permissions]（認可と許可）、[Network Access]（ネットワーク アクセス）、[Authorization Profiles]（認可プロファイル）の順に選択
  - [Dictionary Type]（ディクショナリ タイプ）: RADIUS-IETF
  - [RADIUS Attribute]（RADIUS 属性）: Filter-ID
  - [Attribute Type]（属性タイプ）: String
  - [Attribute Value]（属性値）: Raritan:G{KVM_Admin}（KVM_Admin は Dominion KVM Switch でローカルに作成されたグループ名）。大文字と小文字が区別されます。
- セッション状況（日時）の設定（**必須**）– [Policy Elements]（ポリシー要素）、[Session Conditions]（セッション状況）、[Date and Time]（日時）の順に選択
- ネットワーク アクセス認可ポリシーの設定/作成（**必須**）– [Access Policies]（アクセス ポリシー）、[Access Services]（アクセス サービス）、[Default Network Access]（デフォルト ネットワーク アクセス）、[Authorization]（認可）の順に選択

ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、LX は、ユーザのグループの許可に基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性を返すことによって、これらのユーザ グループ名を提供できます。FILTER-ID は、Raritan:G{*GROUP_NAME*} という形式となります。*GROUP_NAME* は、ユーザが属するグループの名前を示す文字列です。

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

GROUP_NAME は、ユーザが属するグループの名前を示す文字列です。Dial Back Number は、ユーザ アカウントに関連付けられている番号で、LX モデムがユーザ アカウントへのダイヤルバックに使用します。

RADIUS 通信交換仕様

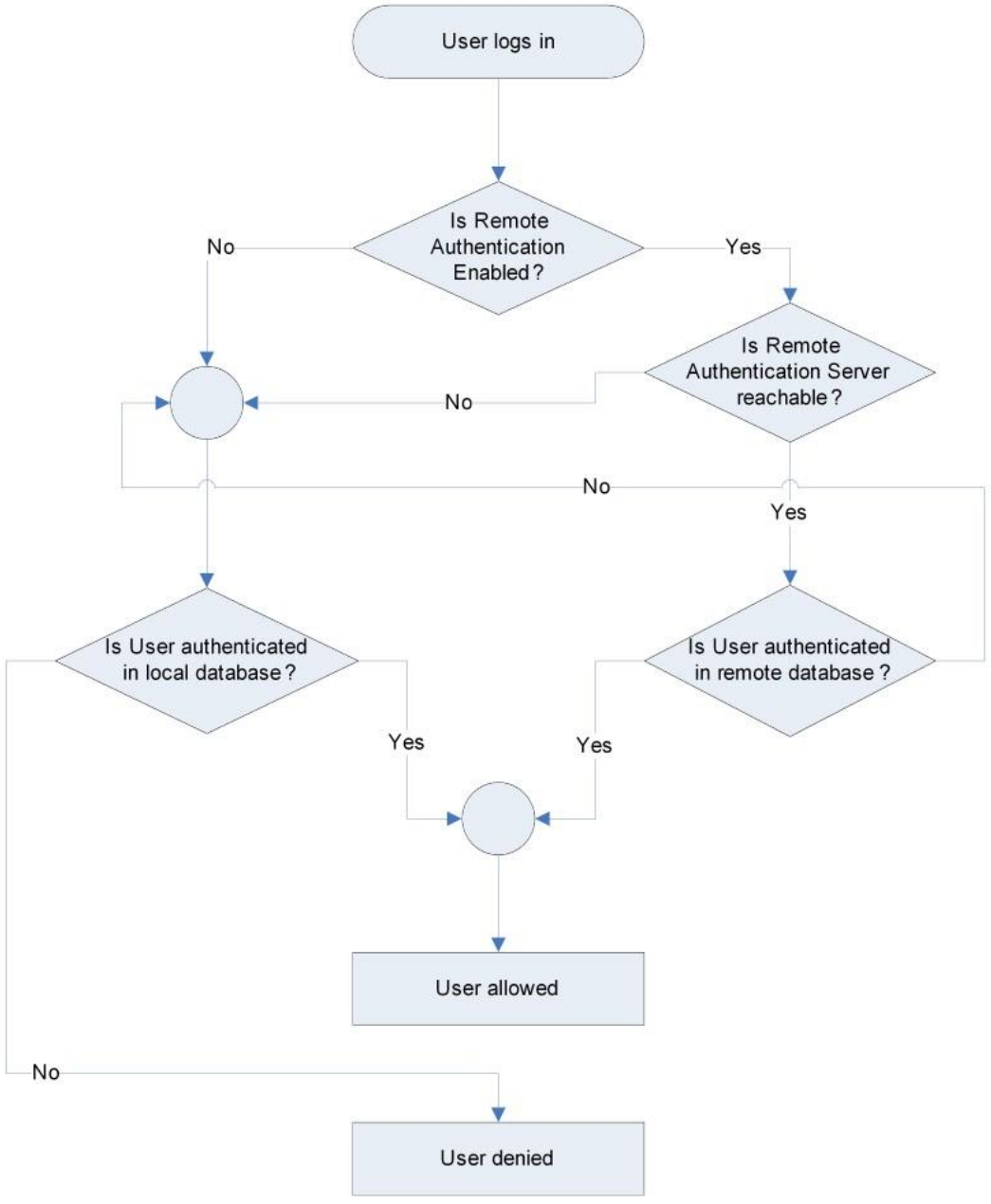
LX は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	LX の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	LX の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

属性	データ
ログアウト	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	LX の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

ユーザ認証プロセス

リモート認証は、その後のフローチャートに指定されたプロセスに従います。

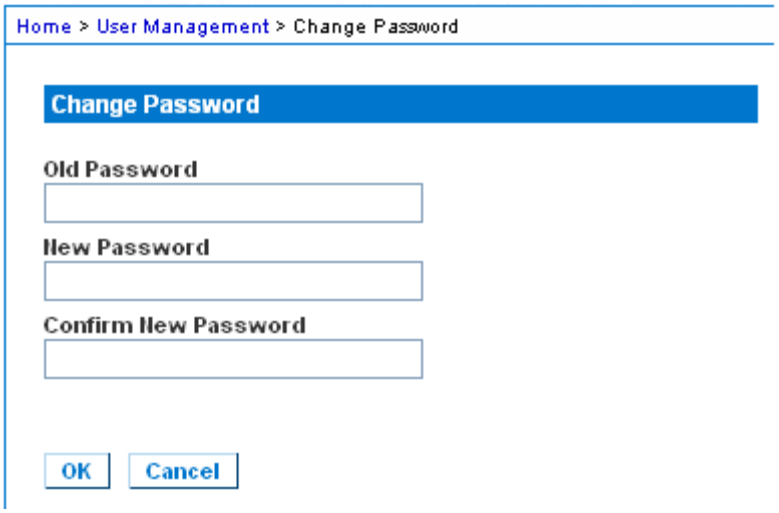


パスワードの変更

▶ **パスワードを変更するには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Change Password] (パスワードの変更) を選択します。[Change Password] (パスワードの変更) ページが開きます。
2. [Old Password] (旧パスワード) フィールドに現在のパスワードを入力します。
3. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力します。[Confirm New Password] (新しいパスワードの確認) フィールドにパスワードを再入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
4. [OK] (OK) をクリックします。
5. パスワードが正常に変更された旨のメッセージが表示されます。[OK] (OK) をクリックします。

注: 強力なパスワードが使用されている場合は、パスワードに必要な形式に関する情報がこのページに表示されます。パスワードと強力なパスワードについての詳細は、「[Strong Passwords] (強力なパスワード)*」**『156p. の "*[強力なパスワード]*" 参照 』**」を参照してください。*



Ch 6 デバイス管理

この章の内容

ネットワーク設定

[Network Settings] (ネットワーク設定) ページを使用して、LX のネットワーク設定 (たとえば、IP アドレス、検出ポート、LAN インタフェース パラメータなど) をカスタマイズします。

IP 設定を行うには 2 つのオプションがあります。

- [None] (なし) (デフォルト) – 推奨されるオプションです (静的 IP)。LX はネットワーク インフラストラクチャの一部であるため、IP アドレスを頻繁に変更されると手間がかかります。このオプションにより、ネットワーク パラメータを固定できます。
- [DHCP] (DHCP) – DHCP サーバによって IP アドレスが自動的に割り当てられます。

▶ ネットワーク設定を変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. ネットワーク基本設定を更新します。「*ネットワーク基本設定* 『*129*p. 』」を参照してください。
3. LAN インタフェースの設定を更新します。「LAN インタフェース設定」を参照してください。
4. [OK] (OK) をクリックして、これらの設定を保存します。変更を適用するために再起動が必要な場合は、再起動メッセージが表示されます。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

ネットワーク基本設定

ここでは、[ネットワーク設定] ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作の詳細については、「*ネットワーク設定* 『*128*p. 』」を参照してください。

▶ IP アドレスを割り当てるには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. LX デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。
   e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。
   - [None] (なし) (静的 IP) - このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

     LX はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。
   - [DHCP] (DHCP) - DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

     このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。
4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。
   a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。

b. [Global/Unique IP Address]（グローバル/一意の IP アドレス）を入力します。これは、LX に割り当てられる IP アドレスです。

c. [Prefix Length]（固定長）を入力します。これは、IPv6 アドレスで使用されるビット数です。

d. [Gateway IP Address]（ゲートウェイ IP アドレス）を入力します。

e. [Link-Local IP Address]（リンク - ローカル IP アドレス）。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索で、またはルータが存在しない場合に使用されます。
[Read-Only]（読み取り専用）

f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。**[Read-Only]（読み取り専用）**

g. [IP Auto Configuration]（IP 自動設定）を選択します。次のオプションを使用できます。

- [None]（設定しない）- 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します（静的 IP）。推奨されるデフォルトのオプションです。

  [IP auto configuration]（IP 自動設定）で [None]（設定しない）を選択すると、[Network Basic Settings]（ネットワーク基本設定）フィールド（[Global/Unique IP Address]（グローバル/一意の IP アドレス）、[Prefix Length]（固定長）、[Gateway IP Address]（ゲートウェイ IP アドレス））が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery]（ルータ検出）- このオプションを使用して、直接接続されるサブネットにのみ適用される [Link Local]（リンクローカル）を超える [Global]（グローバル）または [Unique Local]（一意ローカル）を意味する IPv6 アドレスを自動的に割り当てます。

5. [DHCP]（DHCP）が選択されており、[Obtain DNS Server Address]（DNS サーバ アドレスを取得する）が有効になっている場合は、[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得する）を選択します。[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得する）を選択した場合は、DHCP サーバから得られた DNS 情報が使用されます。

6. [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用する）が選択されている場合は、[DHCP]（DHCP）が選択されているかどうかにかかわらず、このセクションに入力したアドレスを使用して DNS サーバに接続されます。

   [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用する）が選択されている場合は、以下の情報を入力します。これらのアドレスは、停電のためにプライマリ DNS サーバ接続が失われた場合に使用されるプライマリおよびセカンダリの DNS アドレスです。

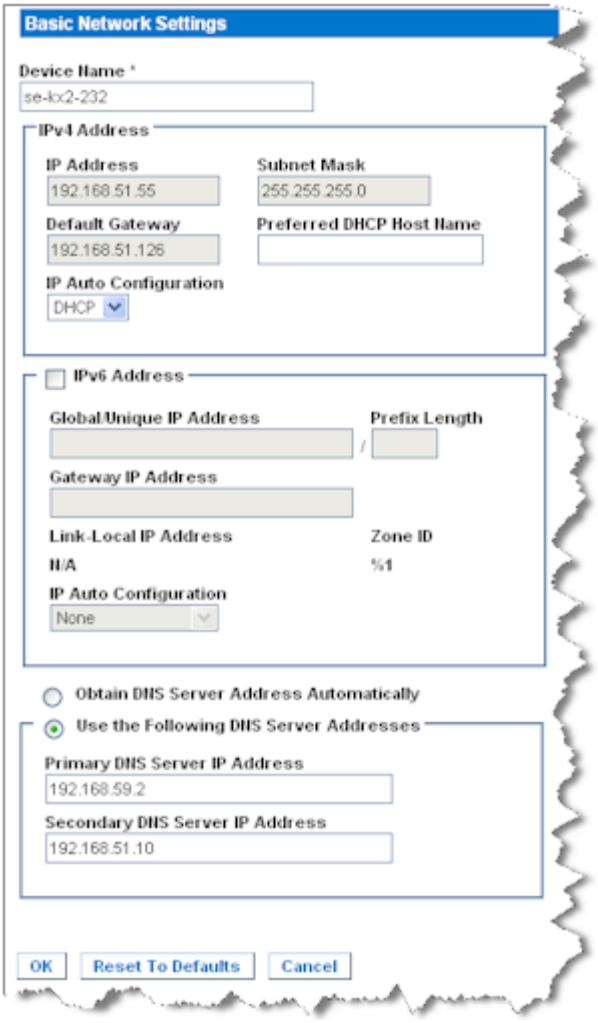
a. プライマリ DNS サーバ IP アドレス
b. セカンダリ DNS サーバ IP アドレス

7. 完了したら［OK］をクリックします。

［ネットワーク設定］ページのこのセクションの設定については、「LAN インタフェース設定」を参照してください。

---

*注: 一部の環境では、［LAN Interface Speed & Duplex］(LAN インタフェースの速度と二重化) のデフォルトである［Autodetect］(自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、LX の［LAN Interface Speed & Duplex］(LAN インタフェースの速度と二重化) フィールドを［100 Mbps/Full Duplex］(またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細については、「***ネットワーク設定*** *『128p. 』」を参照してください。*



LAN インタフェース設定

現在のパラメータ設定は、[現在の LAN インタフェース パラメータ] フィールドで確認します。

1. [デバイス設定] の [ネットワーク] を選択します。[ネットワーク設定] ページが開きます。
2. 以下の [LAN インタフェースの速度と二重化] のオプションから適切なものを選択します。
   - [自動検出] (デフォルト オプション)
   - [10 Mbps/半二重]: 両方の LED が点滅
   - [10 Mbps/全二重]: 両方の LED が点滅
   - [100 Mbps/半二重]: 黄色の LED が点滅
   - [100 Mbps/半二重]: 黄色の LED が点滅
   - [1000 Mbps/全二重] (ギガビット): 緑色の LED が点滅
   - [半二重] の場合、双方向の通信は可能ですが、一度に通信できるのは一方向だけです (同時に通信できません)。
   - [全二重] の場合、同時に双方向の通信が可能です。

注: 半二重または全二重で 10 Mbps で実行しているときに、問題が発生する場合があります。問題が発生した場合は、別の速度と二重化の設定を選択してください。

詳細については、「*Network Speed Settings* 『*216*p. の*"ネットワーク速度の設定"*参照 』」を参照してください。

3. 帯域幅を選択します。
4. [OK] をクリックして LAN 設定を適用します。

デバイス サービス

[デバイス サービス] ページでは、次のことができます。

- SSH アクセスを有効にする。
- ベース LX に対してカスケード接続を有効にする。
- 検出ポートを入力する。
- ダイレクト ポート アクセスを有効にする。
- AKC を使用している場合に、AKC ダウンロード サーバ証明書の検証を有効にする。

SSH を有効にする

管理者が SSH v2 アプリケーションを使用して LX にアクセスできるようにするには、[Enable SSH Access](SSH アクセスを有効にする) チェック ボックスをオンにします。

SSH アクセスを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable SSH Access](SSH アクセスを有効にする) を選択します。
3. [SSH Port Information](SSH ポート情報) を入力します。標準の SSH TCP ポート番号は 22 ですが、ポート番号を変更して高いレベルのセキュリティ処理を提供することもできます。
4. [OK](OK) をクリックします。

HTTP ポートおよび HTTPS ポートの設定

LX によって使用される HTTP ポートまたは HTTPS ポートを設定できるようになりました。 たとえば、デフォルトの HTTP ポートであるポート 80 を別の用途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

HTTP ポートまたは HTTPS ポートの設定を変更するには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [HTTP Port](HTTP ポート) フィールドまたは [HTTPS Port](HTTPS ポート) フィールド (あるいはその両方) に新しいポート番号を入力します。
3. [OK](OK) をクリックします。

検出ポートを入力する

LX の検出は、設定可能な 1 つの TCP ポートで行われます。デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう設定してもかまいません。ファイアウォールの外側から LX にアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

▶ 検出ポートを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Discovery Port] (検出ポート) を入力します。
3. [OK] (OK) をクリックします。

カスケード接続の設定および有効化

LX および汎用カスケード接続は、LX でサポートされています。カスケード接続機能を利用した場合、1 台のベース LX デバイスを介して LX ターゲットにアクセスできます。

注: ベース デバイスとカスケード接続デバイスはすべて同じファームウェア リビジョンで動作している必要があります。

必要に応じて、カスケード接続構成にデバイスを追加したり、カスケード接続構成からデバイスを削除したりできます。カスケード接続レベルは最大 2 段階です。

デバイスをセットアップする際、特定のカスケード接続構成に対して特定の CIM を使用します。カスケード接続構成に追加できるターゲット、CIM の互換性、およびデバイス設定情報については、「***カスケード接続: ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成*** 『***136***p. 』」を参照してください。

カスケード接続デバイスを追加する前に、ベース デバイスおよびカスケード接続デバイスにおいてカスケード接続を有効にする必要があります。ベース デバイスでカスケード接続を有効にするには、[デバイス設定] ページを使用します。カスケード接続デバイスでカスケード接続を有効にするには、[ローカル ポート設定] ページを使用します。デバイスに対してカスケード接続を有効化および設定すると、それらのデバイスが [ポート アクセス] ページに表示されます（「***[ポート アクセス] ページ*** 『***45***p. 』」を参照)。

LX をベース デバイスまたはカスケード接続デバイスとして機能するように設定すると、そのデバイスは次のように表示されます。

- ベース デバイスとして設定した場合、LX 画面の左パネルの [デバイス情報] セクションに、[ベース デバイスとして設定] と表示されます。
- カスケード接続デバイスとして設定した場合、LX 画面の左パネルの [デバイス情報] セクションに、[カスケード接続デバイスとして設定] と表示されます。
- ベース デバイスは、カスケード接続デバイスの画面の左パネルの [接続しているユーザ] の下で [ベース] として表示されます。
- ベース デバイスのカスケード接続ポートに接続しているターゲットは、2 つのポートに接続しているように表示されます。

ベース デバイスからは、[ポート アクセス] ページに表示されている統合ポート リストを使用して、リモート アクセスおよびローカル アクセスできます。カスケード接続デバイスからは、そのデバイスのポート リストを使用してリモート アクセスできます。カスケード接続が有効になっている場合、カスケード接続デバイスからローカル アクセスすることはできません。

CIM 名の変更をはじめとするポート設定は、各デバイスから直接行う必要があります。カスケード接続ターゲット ポートに対する設定は、ベース デバイスから行うことはできません。

カスケード接続構成では、KVM スイッチを使用してサーバを切り替えることもできます。「*KVM スイッチを設定する 『147*p. の*"KVM スイッチの設定"*参照 』」を参照してください。

カスケード接続の有効化

ベース LX デバイスのターゲット サーバ ポートとカスケード接続 LX デバイスのローカル アクセス ポート（ビデオ/キーボード/マウス ポート）を、D2CIM-DVUSB で接続します。

▶ ティアー接続を有効にするには

1. ティアー接続構成内のベース デバイスで、[Device Settings]（デバイス設定）の [Device Services]（デバイス サービス）を選択します。[Device Services Settings]（デバイス サービス設定）ページが表示されます。
2. [Enable Tiering as Base]（ベースとしてのティアー接続を有効にする）を選択します。
3. [Base Secret]（ベース秘密ワード）フィールドに、ベース デバイスとティアー接続デバイスの間で共有される秘密ワードを入力します。この秘密ワードは、ティアー接続デバイスでベース デバイスを認証する際に必要となります。同じ秘密ワードをティアー接続デバイスに対して入力します。
4. [OK]（OK）をクリックします。
5. ティアー接続デバイスを有効にします。ティアー接続デバイスで、[Device Settings]（デバイス設定）の [Local Port Settings]（ローカル ポート設定）を選択します。
6. このページの [Enable Local Ports]（ローカル ポートを有効にする）セクションで、[Enable Local Port Device Tiering]（ローカル ポート デバイスのティアー接続を有効にする）を選択します。
7. [Tier Secret]（ティアー接続秘密ワード）フィールドに、ベース デバイスの [Device Settings]（デバイス設定）ページで入力したのと同じ秘密ワードを入力します。
8. [OK]（OK）をクリックします。

カスケード接続: ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成

CIM 名の変更をはじめとするポート設定は、各デバイスから直接行う必要があります。カスケード接続ターゲット ポートに対する設定は、ベース デバイスから行うことはできません。

カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能

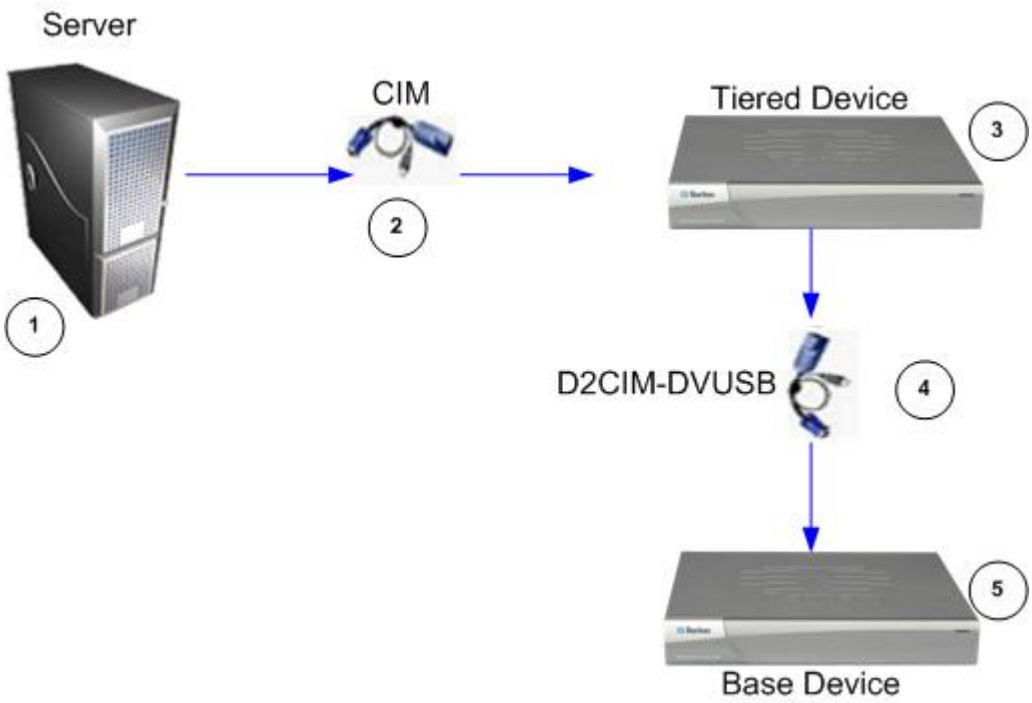
カスケード接続ターゲットでサポートされていない機能は次のとおりです。

- 仮想メディア
- MCCAT

カスケード接続構成における接続例

次の図に、カスケード接続 LX デバイスとベース LX デバイスの接続例を示します。

ベース LX デバイスのターゲット サーバ ポートとカスケード接続 LX デバイスのローカル アクセス ポート（ビデオ/キーボード/マウス ポート）を、D2CIM-DVUSB で接続します。



図の説明	
1	ターゲット サーバ
2	ターゲット サーバとカスケード接続 LX デバイスを接続する CIM

図の説明	
3	カスケード接続 LX デバイス
4	カスケード接続 LX デバイスとベース LX デバイスを接続する D2CIM-DVUSB CIM
5	ベース LX デバイス

URL を経由したダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスにより、ユーザは、デバイスの [Login](ログイン) ダイアログ ボックスおよび [Port Access](ポート アクセス) ページを使用しなくても済むようになります。この機能では、URL でユーザ名とパスワードが指定されていない場合に、ユーザ名とパスワードを直接入力してターゲットに進むこともできます。

以下に、ダイレクト ポート アクセスに関する重要な URL 情報を示します。

VKC およびダイレクト ポート アクセスを使用している場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

AKC とダイレクト ポート アクセスを使用する場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

説明:

- username と password はオプションです。指定しない場合はログイン ダイアログ ボックスが表示され、認証後、ユーザはターゲットに直接接続されます。
- port には、ポート番号またはポート名を指定できます。ポート名を使用する場合は、一意の名前にしなければ、エラーが報告されます。port を省略した場合もエラーが報告されます。
- client=akc は、AKC クライアントを使用しない場合はオプションです。client=akc を指定しない場合、VKC がクライアントとして使用されます。

▶ **ダイレクト ポート アクセスを有効するには、以下の手順に従います。**

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. URL で必要なパラメータを渡してユーザに Dominion デバイス経由でターゲットに直接アクセスさせる場合は、[Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) を選択します。
3. [OK] をクリックします。

AKC ダウンロード サーバ証明書の検証の有効化

AKC クライアントを使用する場合は、[AKC ダウンロード サーバ証明書の検証を有効にする] 機能を使用するかどうかを選択できます。

オプション 1: AKC ダウンロード サーバ証明書の検証を有効にしない (デフォルト設定)

AKC ダウンロード サーバ証明書の検証を有効にしない場合は、以下の操作を行います。すべての Dominion デバイス ユーザは、以下のようにする必要があります。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

オプション 2: AKC ダウンロード サーバ証明書の検証を有効にする

AKC ダウンロード サーバ証明書の検証を有効にする場合は、以下の操作を行います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

▶ **Windows Vista® または Windows 7® を使用する場合、自己署名証明書をインストールするには、以下の手順に従います。**

1. [信頼済みサイト] ゾーンに LX の IP アドレスを追加し、保護モードがオフになっていることを確認します。
2. URL に LX の IP アドレスを使用して Internet Explorer® を起動します。証明書エラー メッセージが表示されます。
3. [証明書の表示] を選択します。
4. [全般] タブで、[証明書のインストール] をクリックします。証明書が信頼されたルート証明機関ストアにインストールされます。
5. 証明書のインストール後、LX の IP アドレスを [信頼済みサイト] ゾーンから削除する必要があります。

▶ **AKC ダウンロード サーバ証明書の検証を有効にするには、以下の手順に従います。**

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。

2. [AKC ダウンロード サーバ証明書の検証を有効にする] チェックボックスをオンにします。なお、この機能は無効のままにしておくこともできます (デフォルト設定は無効)。
3. [OK] をクリックします。

モデムの設定

▶ **モデムを設定するには、以下の手順に従います。**

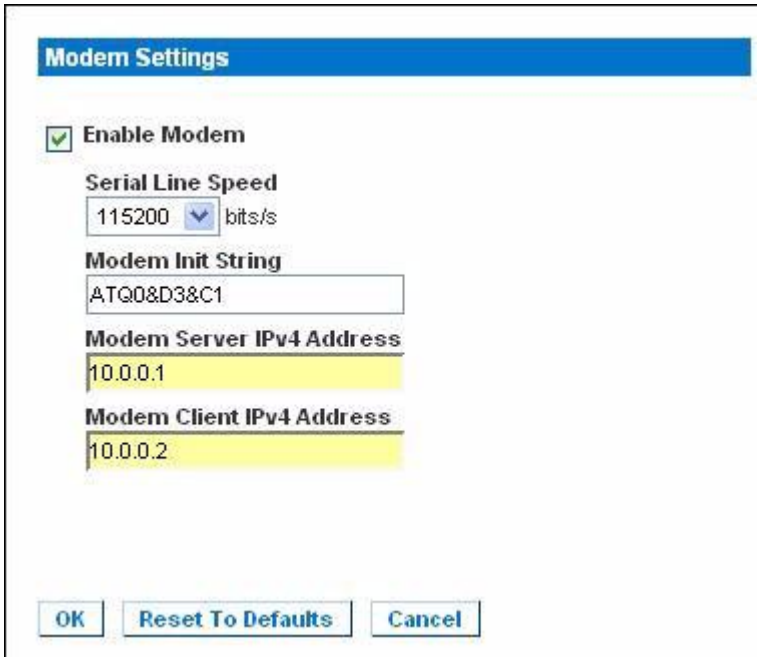
1. [デバイス設定] の [モデム設定] をクリックし、[モデム設定] ページを開きます。
2. [モデムを有効にする] チェックボックスをオンにします。これで、[シリアル ライン速度] フィールドと [モデム Init] フィールドが有効になります。
3. モデムの [シリアル ライン速度] は 11520 に設定されます。
4. [モデム Init 文字列] フィールドにモデム初期化文字列を入力します。モデム文字列を空白のままにすると、デフォルトで、文字列「ATZ OK AT OK」がモデムに送信されます。

   この情報がモデムの設定に使用されます。 以下の値の設定方法はモデムの種類によってさまざまなので、このドキュメントでは、これらの値の設定方法は指定しません。モデム固有の適切な設定を作成するには、モデムを参照する必要があります。

   a. [モデム設定]:
      - RTS/CTS フロー制御を有効にします。
      - RTS 受信時にコンピュータにデータを送信します。
      - CTS は、必要な場合にフロー制御によって切断だけ行うように設定する必要があります。
      - DTR は、DTR トグルでリセットするようにモデムに対して設定する必要があります。
      - DSR は常にオンに設定する必要があります。
      - DCD は、キャリア信号の検出後に有効にするように設定する必要があります (つまり、DCD はリモート側とのモデム接続が確立されたときにのみ有効にする必要があります)。
5. [モデム サーバの IPv4 アドレス] フィールドに IPv4 モデム サーバ アドレスを入力し、[モデム クライアントの IPv4 アドレス] フィールドにクライアント モデム アドレスを入力します。

注: モデム クライアントおよびサーバの IP アドレスは、同じサブネット上にある必要があり、デバイスのサブネットとオーバーラップすることはできません。

6. [OK] をクリックして変更を確認するか、[デフォルトに戻す] をクリックして設定をデフォルトに戻します。



LX で使用するに認定済みのモデムの詳細については、「*認定モデム*『*211*p. 』」を参照してください。モデムを介して LX に接続する場合の最適なパフォーマンスを確保する設定の詳細については、『KVM and Serial Access Clients Guide』の「Creating, Modifying and Deleting Profiles in MPC – Generation 2 Devices」を参照してください。

注: LX HTML インタフェースへの直接モデム アクセスはサポートされていません。モデムを介して LX にアクセスするには、スタンドアロン MPC を使用する必要があります。

日付/時刻の設定

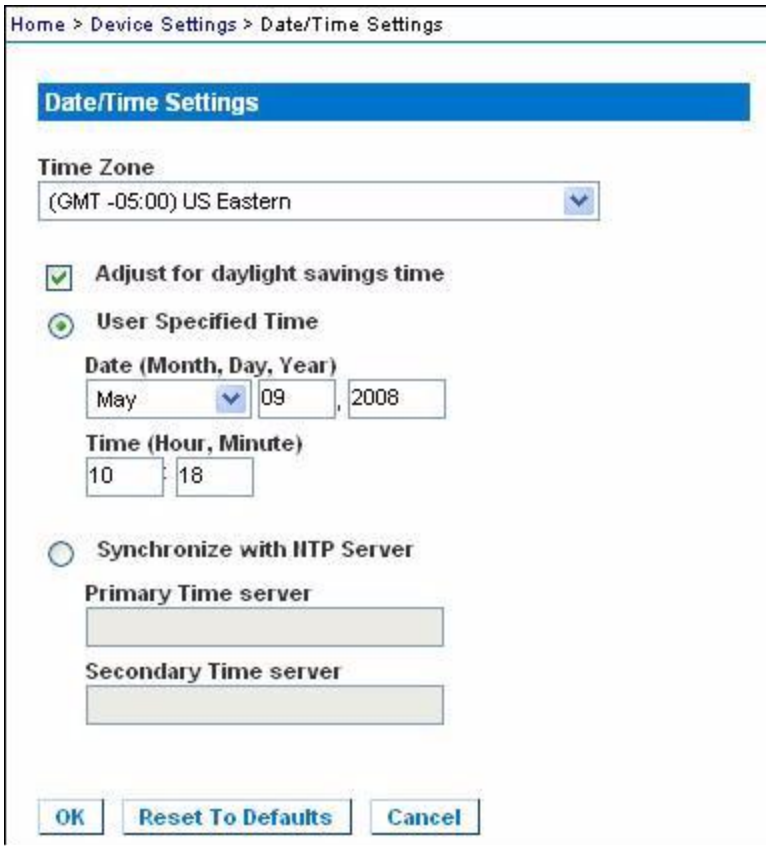
[日付/時刻の設定] ページを使用して、LX の日付と時刻を指定します。これには 2 とおりの方法があります。

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する。

▶ 日付と時刻を設定するには、以下の手順に従います。

1. [デバイス設定] の [日付/時刻] を選択します。[日付/時刻の設定] ページが開きます。
2. [タイム ゾーン] ドロップダウン リストから適切なタイム ゾーンを選択します。

3. 夏時間用の調整を行うには、[夏時間用の調整] チェックボックスをオンにします。
4. 日付と時刻の設定で用いる方法を選択します。
   - [ユーザによる時刻定義]: 日付と時刻を手動で入力するには、このオプションを選択します。[ユーザによる時刻定義] オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - [NTP サーバと同期]: 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期するには、このオプションを選択します。
5. [NTP サーバと同期] オプションを選択した場合は、以下の手順に従います。
   a. プライマリ タイム サーバの IP アドレスを入力します。
   b. セカンダリ タイム サーバの IP アドレスを入力します。**(オプション)**
6. [OK] をクリックします。



イベント管理

LX イベント管理機能によって、SNMP マネージャ、Syslog、監査ログへのシステム イベントの送信を有効または無効にすることができます。

[イベント管理 - 設定] の設定

SNMP の設定

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御し、ネットワーク デバイスとその機能を監視するためのプロトコルです。LX では、イベント管理を通じて SNMP エージェントがサポートされます。

▶ SNMP を設定する (SNMP のログ作成を有効にする) には、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。
2. [SNMP Logging Enabled] (SNMP ログを有効にする) を選択します。これにより、残りの SNMP フィールドが有効になります。
3. [Name] (名前) フィールドには、LX コンソール インタフェースに表示されているとおりに SNMP エージェントの名前 (つまりデバイスの名前) を、[Contact] (連絡先) フィールドには、このデバイスに関連する連絡先名を、[Location] (所在地) フィールドには、Dominion デバイスが物理的に設置されている場所を入力します。
4. [Agent Community String] (エージェント コミュニティの文字列) (デバイスの文字列) を入力します。SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステーションが所属するグループのことです。SNMP コミュニティは、情報の送信先を定義するのに役立ちます。コミュニティ名は、グループを識別するために使用されます。SNMP デバイスや SNMP エージェントは、複数の SNMP コミュニティに所属できます。
5. [Type] (タイプ) ドロップダウン リストを使用して、コミュニティに [Read-Only] (読み取り専用) または [Read-Write] (読み取り/書き込み可能) を指定します。
6. [Destination IP/Hostname] (送信先 IP/ホスト名)、[Port #] (ポート番号)、[Community] (コミュニティ) を指定して、最大で 5 つの SNMP マネージャを設定します。
7. [Click here to view the Dominion SNMP MIB] (Dominion SNMP MIB を表示するにはここをクリックします) というリンクをクリックして、SNMP Management Information Base にアクセスします。
8. [OK] をクリックします。

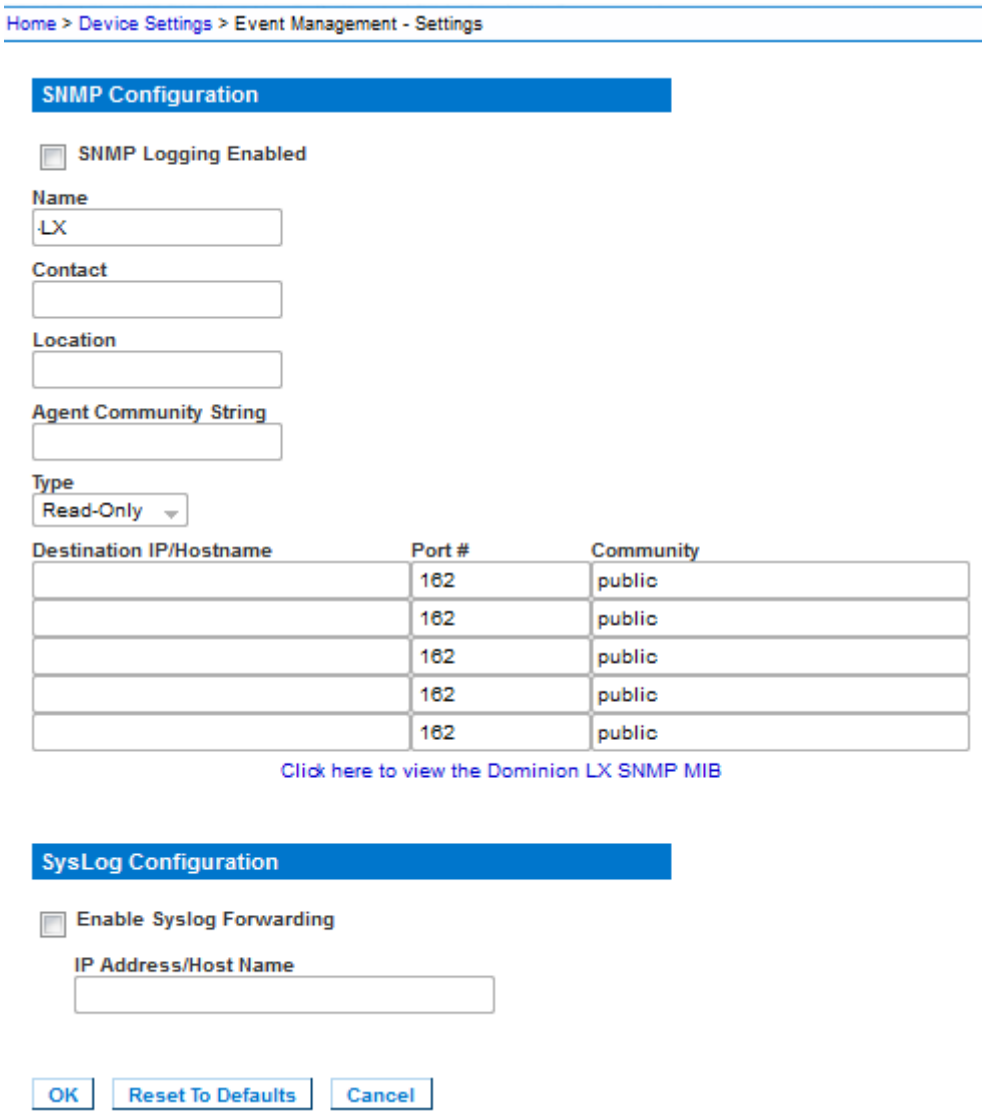
Syslog を設定する (Syslog の送信を有効にする) には、以下の手順に従います。

1. [Enable Syslog Forwarding] (Syslog 送信有効) を選択して、リモート Syslog サーバにデバイス メッセージのログを送信します。
2. [IP Address] (IP アドレス) フィールドに Syslog サーバの IP アドレス/ホスト名を入力します。
3. [OK] をクリックします。

工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

注: IPv6 アドレスでは、ホスト名が最大 80 文字です。



ポートの設定

[ポート設定] ページには、LX のポートの一覧が表示されます。KVM ターゲット サーバに接続されているポートは青色で表示されます。CIM が接続されていないか、CIM 名が空白になっているポートには、デフォルト ポート名「Dominion-LX_Port#」が割り当てられます。「Port#」は LX の物理ポートの番号を表します。

ポートのステータスがダウンである場合、ステータスとして「使用不可」が表示されます。ポートの CIM が削除されているか電源が切られている場合、ポートがダウンになる可能性があります。

ポートの名前を変更した後でも、[デフォルトに戻す] を使用すれば、いつでもデフォルトのポート名に戻ります。

▶ ポート設定にアクセスするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。

   最初このページはポートの番号順に表示されますが、列の見出しをクリックしてフィールドごとに並べ替えられます。

   - [Port Number] (ポート番号) - 1 から LX デバイスで使用できるポートの合計数までの番号が振られています。
   - [ポート名]: ポートに割り当てられている名前です。または、現在 CIM を介して LX に接続されていないため [使用不可] ステータスになっているポートの名前を変更します。[使用不可] ステータスのポートの名前を変更するには、以下のいずれかの手順に従います。
     - ポートの名前を変更します。CIM が接続されると、その CIM 名が使用されます。
     - ポート名を変更し、[次回の CIM 挿入時に名前を維持] を選択します。CIM が接続されると、割り当てられている名前が CIM にコピーされます。
     - [デフォルトに戻す] を選択して、ポート (名前を含む) を工場出荷時のデフォルトに戻します。CIM が接続されると、その CIM 名が使用されます。

   注: ポート (CIM) 名にアポストロフィ (" ' ") を使用することはできません。

   - ポート タイプ:

- [DCIM]: Dominion CIM
- [使用不可]: CIM を接続できません
- [MCUTP]: マスタ コンソール MCUTP、ケーブル内の CIM
- [PCIM]: Paragon CIM
- [デュアル – VM]: 仮想メディア CIM (D2CIM-VUSB および D2CIM-DVUSB)
- [KVM スイッチ]: 汎用 KVM スイッチ接続

2. 編集するポートの [ポート名] をクリックします。[ポート] ページが開きます。

標準ターゲット サーバの設定

▶ **ターゲット サーバに名前を付けるには、以下の手順に従います。**

1. まだすべてのターゲット サーバを接続していない場合は、接続します。装置の接続方法の詳細は、「*手順 3: 装置の接続* 『*28*p. 』」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
3. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
4. ポートのサブタイプとして [標準 KVM ポート] を選択します。
5. 当該ポートに接続されているサーバを識別するための名前を割り当てます。名前には最大 32 文字の英数字と特殊文字を使用できます。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。
8. [OK] をクリックします。

KVM スイッチの設定

LX を使用すると、ホット キー切り替えをサポートしている汎用アナログ KVM スイッチにカスケード接続できます。選択するためのさまざまな KVM ホットキー シーケンスが用意されています。このポート経由で接続されているアナログ KVM スイッチで使用できるホットキー シーケンスと一致するものを選択します。そうすると、カスケード接続のアナログ KVM スイッチに接続されているターゲットに [ポート アクセス] ページの統合ポート リストからアクセスできるようになります。

重要: 作成する KVM スイッチがユーザ グループに表示されるように

するには、まずスイッチを作成してから、グループを作成する必要があります。作成中の KVM スイッチが既存のユーザ グループに表示されるようにする必要がある場合は、ユーザ グループを再作成する必要があります。

KVM スイッチを設定するには、以下の手順に従います。

1. [デバイス設定] の [ポート設定] を選択します。[ポート設定] ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[ポート] ページが開きます。
3. [KVM スイッチ] を選択します。
4. KVM スイッチのモデルを選択します。

   注: ドロップダウン リストにはスイッチが 1 つしか表示されません。
5. [KVM 切り替えホット キー シーケンス] を選択します。
6. ターゲット ポートの最大数を 2 ～ 32 の範囲で入力します。
7. [KVM スイッチ名] フィールドに、このポート接続を参照する際に使用する名前を入力します。
8. KVM スイッチ ホット キー シーケンスを適用するターゲットをアクティブ化します。KVM スイッチ ポートにターゲットが接続されていることを示すため、各ポートに対して [アクティブ] を選択します。
9. このページの [KVM 管理下リンク] セクションで、Web ブラウザ インタフェースを使用できる場合にその Web ブラウザ インタフェースへの接続を設定できます。
   a. [アクティブ]: 設定されたリンクをアクティブにするには、[アクティブ] チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[アクティブ] チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[アクティブ] チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL 名]: インタフェースの URL を入力します。
   c. [ユーザ名]: インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [パスワード]: インタフェースへのアクセスに使用されるパスワードを入力します。

e. [Username Field] (ユーザ名フィールド) – URL で使用されるユーザ名パラメータを入力します。たとえば、「*username*=admin」と入力します。*username* はユーザ名フィールドです。

f. [Password Field] (パスワード フィールド) – URL で使用されるパスワード パラメータを入力します。たとえば、「*passname*=raritan」と入力します。*passname* はパスワード フィールドです。

10. [OK] をクリックします。

KVM スイッチ ポートまたは URL のアクティブ ステータスを変更するには、以下の手順に従います。

1. [デバイス設定] の [ポート設定] を選択します。[ポート設定] ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[ポート] ページが開きます。
3. KVM スイッチ ターゲット ポートまたは URL の [アクティブ] チェック ボックスをオフにし、アクティブ ステータスを変更します。
4. [OK] をクリックします。

LX のローカル ポートの設定

[Local Port Settings] (ローカル ポート設定) ページでは、LX ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。

ローカル ポートに関する設定値をカスタマイズするには

注: [Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. 標準ローカル ポートを有効にするには、[標準ローカル ポートを有効にする] チェック ボックスをオンにします。無効にするにはチェックボックスをオフにします。デフォルトでは、標準ローカル ポートは有効になっていますが、必要に応じて無効にすることができます。この設定を変更すると、ブラウザが再起動します。 カスケード接続機能を利用する場合、この機能は無効になります。両方の機能を同時に利用することができないからです。

3. カスケード接続機能を利用する場合、[ローカル ポート デバイスのカスケード接続を有効にする] チェック ボックスをオンにし、[カスケード接続秘密ワード] フィールドにカスケード接続秘密ワードを入力します。カスケード接続を設定するには、[デバイス サービス] ページでベース デバイスを設定する必要があります。カスケード接続の詳細については、「*カスケード接続の設定および有効化*『*135*p. 』」を参照してください。
4. 必要な場合は、[ローカル ポート スキャン モード] 設定をカスタマイズします。これらの設定は、[ポート] ページからアクセスされるスキャン設定機能に適用されます。「***ポートのスキャン*** 『*48*p. 』」を参照してください。
   - [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
   - [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
5. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)
   - [United Kingdom] (イギリス英語)
   - [French (France)] (フランス語 (フランス))
   - [German (Germany)] (ドイツ語 (ドイツ))
   - [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
   - [Simplified Chinese] (簡体字中国語)
   - [Traditional Chinese] (繁体字中国語)
   - [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
   - [German (Switzerland)] (ドイツ語 (スイス))
   - [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
   - [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
   - [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
   - [Danish (Denmark)] (デンマーク語 (デンマーク))
   - [Belgian (Belgium)] (ベルギー語 (ベルギー))

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

注: トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

6. [Local Port Hotkey]（ローカル ポート ホットキー）ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに LX ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock]（Scroll Lock キーを 2 回押す）ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock]（Num Lock キーを 2 回押す）	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock]（Caps Lock キーを 2 回押す）	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key]（左 Alt キーを 2 回押す）	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key]（左 Shift キーを 2 回押す）	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key]（左 Ctrl キーを 2 回押す）	左 Ctrl キーをすばやく 2 回押します。

7. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。その後ホットキーを使用して、そのターゲット サーバの画面から LX ローカル コンソールの画面に戻すことができます。接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー シーケンスの例については、「接続キーの例」を参照してください。
8. 必要に応じて、[画面切り替え遅延（秒）] ボックスに 0 ～ 5 秒の範囲の数値を入力します。通常は「0」と入力します。ただし、一部のモニタでは画面切り替えに時間がかかるので、その場合は適切な値を入力します。
9. 省電力機能を利用する場合、次の手順を実行します。
   a. [省電力モード] チェック ボックスをオンにします。
   b. [省電力モードのタイムアウト（分）] ボックスに、省電力モードに移行するまでの時間（単位: 分）を入力します。
10. [解像度] ボックスの一覧で、LX ローカル コンソールの画面解像度を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
    - 800 x 600

- 1024 x 768
- 1280 x 1024

11. [垂直走査周波数（Hz)] ボックスの一覧で垂直走査周波数を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
    - 60 Hz
    - 75 Hz
12. [ローカル ユーザ認証] でローカル ユーザ認証タイプを選択します。
    - [ローカル/LDAP/RADIUS]: これは推奨オプションです。認証の詳細については、「*リモート認証* 『*35*p. 』」を参照してください。
    - [なし]: LX ローカル コンソールからのアクセスに対して認証は行われません。このオプションは、安全な環境でのみ選択することをお勧めします。
13. [OK] をクリックします。

デフォルトの GUI 言語設定の変更

LX の GUI では、以下のローカライズ言語がサポートされています。

- 日本語
- 簡体字中国語
- 繁体字中国語

▶ GUI 言語を変更するには、以下の手順に従います。

1. [デバイス設定] の [言語] を選択します。[言語設定] ページが開きます。
2. [言語] ボックスの一覧で、GUI に適用する言語を選択します。
3. [適用] をクリックします。[デフォルトに戻す] をクリックして、[英語] に戻します。

注: 新しい言語を適用すると、オンライン ヘルプも、選択言語に合わせてローカライズされます。

Ch 7 セキュリティ上の問題

この章の内容

セキュリティ設定

[Security Settings] (セキュリティ設定) ページで、ログオン制限、ユーザ ブロック、パスワード ルール、および暗号化と共有に関する設定を行うことができます。

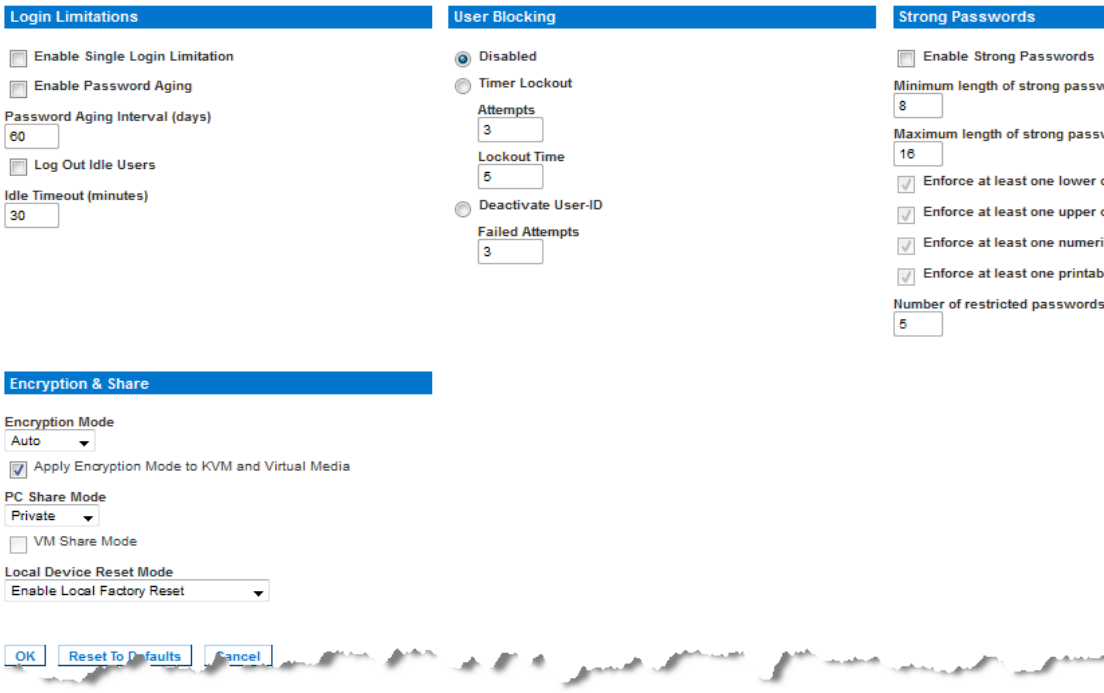
パブリック キーとプライベート キーの交換には Raritan SSL 証明書が使用され、セキュリティのレベルを高めます。Raritan の Web サーバ証明書は自己署名されています。Java アプレット証明書は、VeriSign の証明書によって署名されています。暗号化を行うと、情報が漏洩しないよう保護されていることを保証できます。またこれらの証明書によって、事業体の身元が Raritan, Inc であることが証明されます。

▶ セキュリティ設定を行うには、以下の手順に従います。

1. [Security] (セキュリティ) の [Security Settings] (セキュリティ設定) を選択します。[Security Settings] (セキュリティ設定) ページが開きます。
2. 必要に応じて、*[Login Limitations] (ログイン制限)* 『*154*p. の"*[ログイン制限]*"参照 』 の設定を更新します。
3. 必要に応じて、*[Strong Passwords] (強力なパスワード)* 『*156*p. の"*[強力なパスワード]*"参照 』 の設定を更新します。
4. 必要に応じて、*[User Blocking] (ユーザ ブロック)* 『*157*p. の"*[ユーザ ブロック]*"参照 』 の設定を更新します。
5. 必要に応じて、*[Encryption & Share] (暗号化および共有)* 『*159*p. の"*暗号化および共有*"参照 』 の設定を更新します。
6. [OK] (OK) をクリックします。

▶ デフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

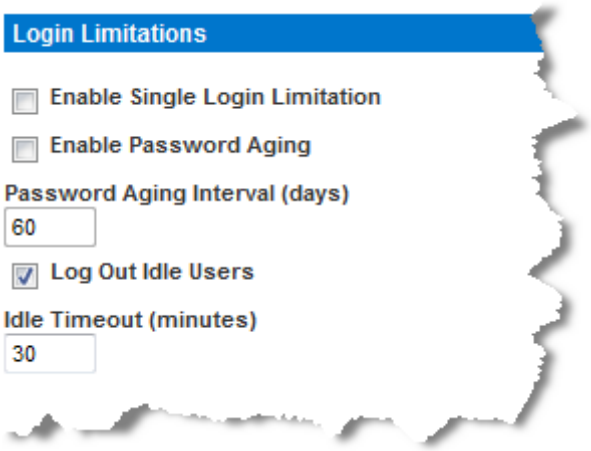


[ログイン制限]

[ログイン制限] セクションでは、シングル ログイン、パスワード エージング、アイドル ユーザのログアウトに関する制限を指定できます。

制限	説明
[シングル ログイン制限を有効にする]	このチェック ボックスをオンにした場合、ユーザ名ごとに同時に 1 人しかログオンできません。このチェック ボックスをオフにした場合、所定のユーザ名とパスワードの組み合わせで、複数のクライアント ワークステーションからデバイスに同時接続できます。
[パスワード エージングを有効にする]	これを選択すると、[パスワード エージング間隔] で指定した日数に基づいて、すべてのユーザに対して定期的にパスワードを変更するよう要求します。 [パスワード エージングを有効にする] チェック ボックスをオンにするとこのフィールドが有効になるため、設定する必要があります。パスワー

制限	説明
	ドの変更が要求される間隔を日数で入力します。デフォルトの日数は 60 日です。
[アイドル ユーザをログアウトする]、[分後（1 ～ 365)]	[アイドル ユーザをログオフする] チェック ボックスをオンにした場合、[分後（1 ～ 365)] ボックスに入力した時間が経過した後にアイドル ユーザが自動ログオフされます。キーボードまたはマウスで操作が行われない場合は、すべてのセッションおよびすべてのリソースがログアウトされます。ただし、実行中の仮想メディア セッションはタイムアウトしません。 [分後（1 ～ 365)] ボックスに入力した時間が経過した後にアイドル ユーザが自動ログアウトされます。このボックスが有効になるのは、[アイドル ユーザをログオフする] チェック ボックスをオンにした場合です。このボックスに入力できる値は 1 ～ 365 の範囲です。



[強力なパスワード]

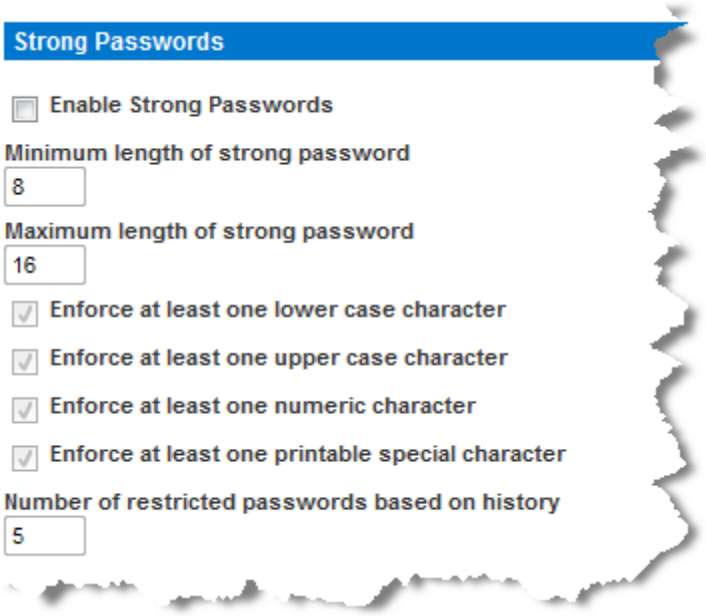
[強力なパスワード] セクションで値を指定すると、このシステムにおけるローカル認証の安全性が高まります。強力なパスワードを使用すると、最小長と最大長、必要な文字、パスワード履歴の保持など、有効な LX ローカル パスワードの形式を設定できます。

強力なパスワードには、アルファベットとアルファベット以外の文字（句読点または数字）をそれぞれ 1 文字以上含むパスワードを指定する必要があります。また、パスワードとユーザ名の最初の 4 文字には同じ文字列を使用できません。

[強力なパスワードを有効にする] チェック ボックスをオンにした場合、強力なパスワードの規則が適用されます。パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログオンする際にパスワードを変更するよう自動的に求められます。[強力なパスワードを有効にする] チェック ボックスをオフにした場合、標準の形式になっているかどうかだけが検査されます。[強力なパスワードを有効にする] チェック ボックスをオンにした場合、次のフィールドが有効になるので、指定する必要があります。

フィールド	説明
[強力なパスワードの最小長]	パスワードは 8 文字以上でなければなりません。デフォルトでは 8 文字ですが、最大 63 文字まで拡張できます。
[強力なパスワードの最大長]	The default is 8 minimum and 16 the is the default maximum. (デフォルトでは 16 文字ですが、最大 64 文字まで拡張できます。)
[1 文字以上の小文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の小文字が必要になります。
[1 文字以上の大文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の大文字が必要になります。
[1 文字以上の数字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の数字が必要になります。
[1 文字以上の印刷可能な特殊文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の印刷可能な特殊文字が必要になります。
[履歴を参照する制限パスワードの数]	このボックスの値は、パスワード履歴の深さ、つまり、繰り返し使用することのできない以前のパスワードの数を意味します。範囲は 1 ～ 12 で、デフォル

フィールド	説明
	トは 5 です。



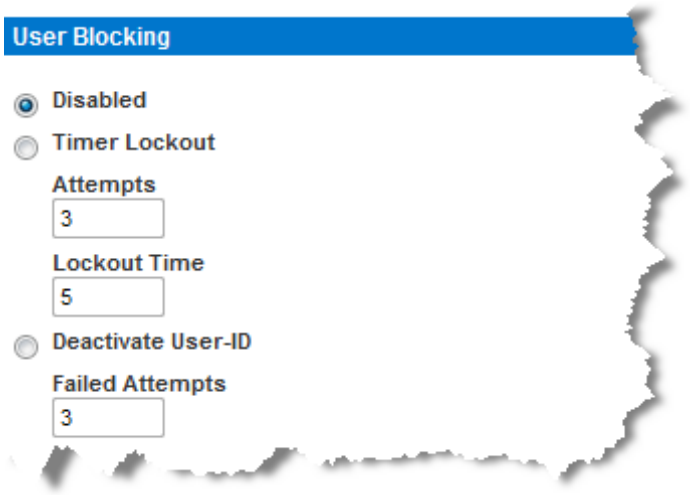
[ユーザ ブロック]

[ユーザ ブロック] セクションでは基準を指定し、ユーザが指定回数ログオンに失敗するとシステムにアクセスできなくなるようにします。

次の 3 つのオプションは、相互に排他的です。

オプション	説明
[無効]	デフォルト値です。認証に失敗した回数に関わらず、ユーザのアクセスはブロックされません。

オプション	説明
[タイマ ロックアウト]	ユーザが指定回数より多くログオンに失敗すると、システムへのアクセスが指定の時間拒否されます。これを選択した場合は次のフィールドが有効になります。 ▪ [試行回数]: この回数より多くログオンに失敗すると、ユーザはロックアウトされます。有効な範囲は 1 ～ 10 で、デフォルトの試行回数は 3 です。 ▪ [ロックアウト時間]: ユーザがロックアウトされる時間です。有効な範囲は 1 ～ 1440 分で、デフォルトでは 5 分です。 *注: [タイマ ロックアウト] で指定した値は、Administrator の役割が割り当てられているユーザには適用されません。*
[ユーザ ID を無効化]	このオプションを選択した場合は、[試行回数] フィールドで指定した回数より多くログオンに失敗すると、ユーザはシステムからロックアウトされます。 ▪ [試行回数]: この回数より多くログオンに失敗すると、そのユーザのユーザ ID が無効になります。このボックスが有効になるのは、[ユーザ ID を無効化] オプションを選択した場合です。有効な範囲は 1 ～ 10 です。 指定回数より多くログオンに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、[ユーザ] ページの [有効化] チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。



暗号化および共有

[Encryption & Share] (暗号化および共有) セクションでは、使用する暗号化のタイプ、PC と VM の共有モード、LX のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

警告: ご使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから LX にアクセスできなくなります。

▶ 暗号化と共有を設定するには、以下の手順に従います。

1. [暗号化モード] ボックスの一覧で暗号化モードを選択します。選択した暗号化モードがご使用のブラウザでサポートされていない場合 LX に接続できない、という内容の警告が表示されます。この警告は、"暗号化モードを選択する際、ご使用のブラウザでその暗号化モードがサポートされていることを確認してください。サポートされていない場合、LX に接続できません" という意味です。

暗号化モード	説明
[自動]	これは推奨オプションです。使用可能な最高強度の暗号化モードに自動設定されます。
[RC4]	RSA RC4 暗号方式を使用して、ユーザ名、パスワード、ビデオ送信を含む KVM データが保護されます。これは、最初の接続認証中に LX とリモート PC 間のプライベート通信チャンネルを提供する 128 ビットの SSL (セキュア ソケット レイヤ) プロトコルで

暗号化モード	説明
	す。
[AES-128]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"128" はキーの長さを意味します。[AES-128] を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「***ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する***『*162*p. の"***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する***"参照 』」を参照してください。
[AES-256]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"256" はキーの長さを意味します。[AES-256] を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「***ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する***『*162*p. の"***ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する***"参照 』」を参照してください。

注: [自動] を選択しなかった場合、MPC は最高強度の暗号化モードに設定されます。

注: Windows XP® (Service Pack 2 適用) と Internet Explorer® 7 を使用している場合、AES-128 暗号化モードで LX にリモート接続することはできません。

2. [Apply Encryption Mode to KVM and Virtual Media] (暗号化モードを KVM および仮想メディアに適用する) チェック ボックスの値を指定します。このチェック ボックスをオンにした場合、選択した暗号化モードが KVM と仮想メディアの両方に適用されます。認証後、KVM データと仮想メディア データが 128 ビットの暗号化モードで転送されます。
3. [PC Share Mode] (PC 共有モード) ボックスの一覧で値を選択します。グローバルな同時リモート KVM アクセスを特定し、最大 8 人までのリモート ユーザが LX に同時にログオンし、デバイスを介してターゲット サーバを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
   - [Private] (プライベート): PC を共有しません。これはデフォルト値です。一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。
   - [PC-Share] (PC 共有): KVM ターゲット サーバに最大 8 人のユーザ (管理者または非管理者) が同時にアクセスできます。ただし、リモート ユーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウスの操作を止めないユーザがいると、制御が不規則になる場合があることに注意してください。
4. 必要に応じて、[VM Share Mode] (VM 共有モード) チェック ボックスをオンにします。このチェック ボックスは [PC-Share Mode] (PC 共有モード) ボックスの一覧で [PC-Share] (PC 共有) を選択した場合にのみ有効になります。このオプションを選択すると、複数のユーザで仮想メディアを共有できるようになります。つまり、複数のユーザが同じ仮想メディア セッションにアクセスできます。デフォルトでは、このチェック ボックスはオフになっています。
5. 必要に応じて、[Local Device Reset Mode] (ローカル デバイス リセット モード) ボックスの一覧で値を選択します。このオプションでは、ユニットの背面にあるハードウェア リセット ボタンが押下された際に実行するアクションを指定します。詳細については、「*リセット ボタンを使用して LX をリセットする* 『*203* p. 』」を参照してください。次のいずれかの値を選択します。

ローカル デバイス リセット モード	説明
[Enable Local Factory Reset] (ローカルで出荷時設定にリセットする) (デフォルト)	LX を出荷時設定にリセットします。
[Enable Local Admin Password Reset] (ローカルで管理者パスワードだけをリセット	ローカルの管理者パスワードだけをリセットします。パスワードは raritan に戻ります。

ローカル デバイス リセット モード	説明
する)	
[Disable All Local Resets] (ローカルでリセットしない)	リセットは一切実行されません。

ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する

LX では AES 256 ビット暗号化方式がサポートされています。ご使用のブラウザで AES がサポートされているかどうか不明な場合は、そのブラウザの製造元に問い合わせるか、または、確認したい暗号化方式を使用してそのブラウザで https://www.fortify.net/sslcheck.html にアクセスしてください。この Web サイトでは、ご使用のブラウザの暗号化方式が検出され、レポートが表示されます。

注: Internet Explorer® 6 では、AES 128 ビットおよび 256 ビット暗号化方式はサポートされていません。

AES (256 ビット) を使用する際の前提条件とサポート対象構成

AES 256 ビット暗号化方式は、次のブラウザでのみサポートされています。

- Firefox® 2.0.0.x および 3.0.x 以降
- Internet Explorer 7 および 8

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java™ Cryptography Extension® (JCE®) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。

各種 JRE™ の管轄ファイルは、次のページの [other downloads] セクションで入手できます。

- JRE1.6: http://java.sun.com/javase/downloads/index_jdk5.jsp

SSL 証明書

LX では、接続先クライアントとの間で送受信されるトラフィックを暗号化するために Secure Sockets Layer (SSL) が使用されます。LX とクライアントとの接続を確立する際、暗号化された証明書を使用して、LX の正当性をクライアントに示す必要があります。

LX 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって署名された証明書をインストールすることができます。CA はまず、CSR 発行元の身元情報を検証します。続いて、署名された証明書を発行元に返します。有名な CA によって署名されたこの証明書は、証明書発行者の身元を保証する目的で使用されます。

注: CSR は、LX 上で生成する必要があります。

▶ SSL 証明書を作成してインストールするには、以下の手順に従います。

1. [セキュリティ] メニューの [セキュリティ証明書] をクリックします。
2. 次の各フィールドの値を指定します。
   a. [共通名]: LX をユーザのネットワークに追加したときに指定した、LX のネットワーク名。通常は完全修飾ドメイン名です。これは、Web ブラウザで LX にアクセスする際に使用する名前から、プレフィックスである http:// を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合、HTTPS を使用して LX にアクセスする際に、ブラウザでセキュリティ警告ダイアログ ボックスが開きます。
   b. [組織内部門]: LX が属する、組織内の部門。
   c. [組織]: LX が属する組織。
   d. [市区町村]: 組織が存在する市区町村。
   e. [都道府県]: 組織が存在する都道府県。
   f. [国 (ISO コード)]: 組織が存在する国。2 文字の ISO コードを入力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」と入力します。
   g. [チャレンジ パスワード]: 一部の CA は、証明書が失効した場合などに証明書の変更を許可するための、チャレンジ パスワードを要求します。このパスワードは 4 文字以上にする必要があります。
   h. [チャレンジ パスワードの確認入力]: 確認のためチャレンジ パスワードを再度入力します。
   i. [電子メール]: LX とそのセキュリティを担当する人の電子メール アドレス。

j. [キー長（単位: ビット)]: 生成されるキーの長さ（単位: ビット)。デフォルト値は [1024] です。

k. [自己署名証明書の作成] チェックボックスを選択します（該当する場合)。

3. [作成] をクリックし、CSR を生成します。

CSR 証明書をダウンロードするには、以下の手順に従います。

1. CSR、および、CSR 生成時に使用された秘密鍵を含むファイルをダウンロードするため、[ダウンロード] をクリックします。

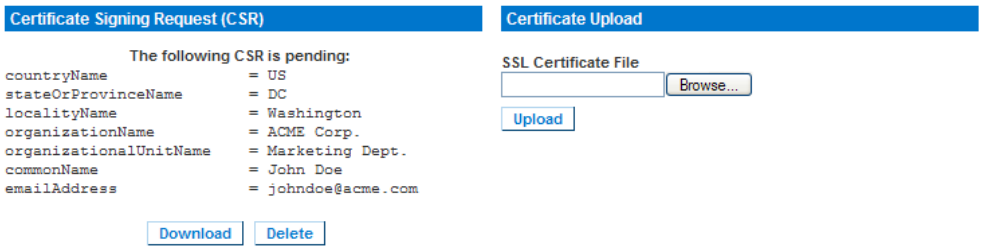
注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。

2. 証明書を取得するため、保存されている CSR を CA に送信します。CA から新しい証明書が届きます。

CSR をアップロードするには、以下の手順に従います。

1. [アップロード] をクリックし、証明書を LX にアップロードします。

注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。



この 3 つの手順が完了すると、LX 専用の証明書が入手されます。この証明書は、LX の身元をクライアントに対して示す際に使用されます。

重要: LX 上の CSR を破棄した場合、復旧する方法はありません。誤って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

Ch 8 保守

この章の内容

[Audit Log] (監査ログ)

LX のシステム イベントに関するログが作成されます。監査ログは最大で約 2K 分のデータを保持でき、これを超えると最も古いエントリから上書きされます。監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、[Device Settings] (デバイス設定) の [Event Management] (イベント管理) ページから設定します。 監査ログおよび Syslog でキャプチャされる内容については、「*監査ログおよび Syslog でキャプチャされるイベント* 『*215*p. 』」を参照してください。

LX の監査ログを表示するには

1. [Maintenance] (保守) メニューの [Audit Log] (監査ログ) をクリックします。[Audit Log] (監査ログ) ページが開きます。

   [Audit Log] (監査ログ) ページでは、日時順にイベントが表示されます (最も新しいイベントが先頭に表示されます)。監査ログに含まれる情報は次のとおりです。

   - [Date] (日時): イベントが発生した日時 (24 時間形式)。
   - [Event] (イベント): [Event Management] (イベント管理) ページに一覧表示されるイベント名。
   - [Description] (説明): イベントの詳細な説明。

監査ログを保存するには

注: 監査ログの保存は LX リモート コンソールでのみ実行できます。LX ローカル コンソールでは実行できません。

1. [Save to File] (ファイルに保存) をクリックします。[Save File] (ファイルに保存) ダイアログ ボックスが開きます。

2. ファイル名と保存先フォルダを選択し、[Save]（保存）をクリックします。監査ログが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

監査ログのページ間を移動するには

- [Older]（古いログへ）リンクおよび [Newer]（新しいログへ）リンクを使用します。

デバイス情報

[デバイス情報] ページには、使用している LX デバイスとコンピュータ インタフェース モジュール (CIM) に関する詳細情報が表示されます。これらの情報は、Raritan のテクニカル サポート部門に問い合わせをする際に役立ちます。

LX と CIM に関する情報を表示するには、以下の手順に従います。

- [保守] メニューの [デバイス情報] をクリックします。[デバイス情報] ページが開きます。

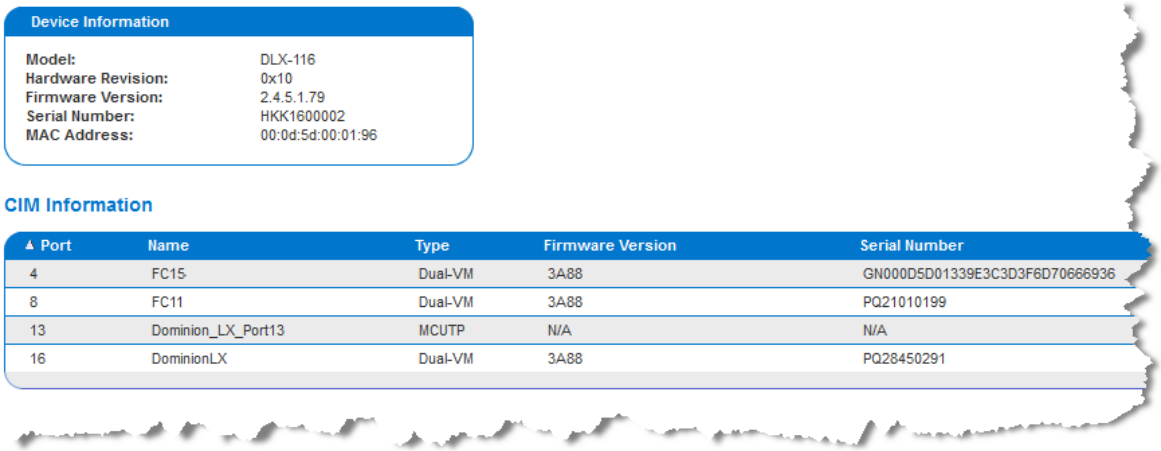
使用している LX に関する以下の情報が提供されます。

- モデル
- ハードウェア リビジョン
- ファームウェア バージョン
- シリアル番号
- MAC アドレス

CIM に関して表示される情報は次のとおりです。

- ポート (番号)
- 名前
- CIM のタイプ: DCIM または VM
- ファームウェア バージョン
- CIM のシリアル番号: この番号は、サポートされている CIM から直接入手できます。

注: DCIM-USB、DCIM-PS2、DCIM-USB G2 の各 CIM の数値部分またはシリアル番号だけが表示されます。たとえば、XXX1234567 が表示されます。フィールドにシリアル番号が設定されている CIM の場合は、シリアル番号プレフィックス GN が表示されます。



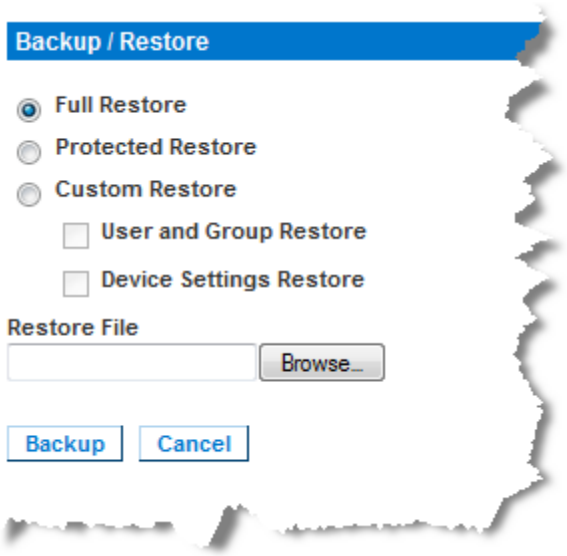
バックアップと復元

[バックアップ/復元] ページでは、LX の設定情報をバックアップおよび復元できます。

バックアップ/復元機能には、業務継続性を確保するというメリットに加え、時間節約効果もあります。たとえば、使用中の LX のユーザ設定情報をバックアップして別の LX に復元することにより、その復元先 LX をすぐに使用できるようになります。また、1 台の LX をセットアップし、その設定情報を複数台の LX にコピーすることもできます。

[バックアップ/復元] ページを開くには、以下の手順に従います。

- [保守] メニューの [バックアップ/復元] をクリックします。[バックアップ/復元] ページが開きます。



注: バックアップ処理では、常にシステム全体がバックアップされます。復元処理では、全体を復元するか一部を復元するかをユーザが選択できます。

Firefox® または Internet Explorer® 5 以前を使用している場合、LX をバックアップするには、以下の手順に従います。

1. [バックアップ] をクリックします。[ファイルのダウンロード] ダイアログ ボックスが開きます。
2. [保存] をクリックします。[名前を付けて保存] ダイアログ ボックスが開きます。
3. 保存先フォルダを選択してファイル名を入力し、[保存] をクリックします。[ダウンロードの完了] ダイアログ ボックスが開きます。

4. [閉じる] をクリックします。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

Internet Explorer 6 以降を使用している場合、LX をバックアップするには、以下の手順に従います。

1. [バックアップ] をクリックします。[開く] ボタンを含む [ファイルのダウンロード] ダイアログ ボックスが開きます。[開く] をクリックしないでください。

   IE 6 以降では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように求められます。これを回避するには、ファイルを開くために使用されるデフォルトのアプリケーションをワードパッド® に変更する必要があります。

2. このためには、以下の手順に従います。
   a. バックアップ ファイルを保存します。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
   b. 保存されたら、ファイルを探して右クリックします。[プロパティ] を選択します。
   c. [全般] タブで [変更] をクリックし、[WordPad] を選択します。

LX を復元するには、以下の手順に従います。

警告: 使用している LX を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。つまり、バックアップ時点での管理者のユーザ名とパスワードを覚えていない場合、LX からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた場合、その IP アドレスも同様に復元されます。IP アドレスの割り当てに DHCP を使用している場合、ローカル ポートにアクセスして復元後の IP アドレスを調べる必要があります。

1. 実行する復元処理のタイプを選択します。
   - [完全復元]: システム全体を復元します。この復元タイプの主な用途は、一般的なバックアップ/復元処理です。
   - [部分復元]: デバイス固有情報 (例: IP アドレス、名前) 以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の LX をセットアップし、その設定情報を複数台の LX にコピーするケースなどが考えられます。
   - [カスタム復元]: この復元タイプを選択した場合、[ユーザとグループの復元] チェック ボックスと [デバイス設定の復元] チェック ボックスのいずれか一方または両方をオンにすることができます。

- [ユーザとグループの復元]: このチェック ボックスをオンにした場合、ユーザ情報とグループ情報だけが復元されます。証明書および秘密鍵ファイルは*復元されません*。別の LX 上でユーザ情報をセットアップする際に便利です。
- [デバイス設定の復元]: デバイス情報をコピーする際に便利です。

2. [参照] をクリックします。[ファイルを選択] ダイアログ ボックスが開きます。
3. 適切なバックアップ ファイルを探して選択し、[開く] をクリックします。選択したファイルが [復元ファイル] ボックスに表示されます。
4. [復元] をクリックします。選択した復元タイプに基づいて、設定情報が復元されます。

CIM のアップグレード

この項で説明する手順に従って、LX のメモリに格納されているファームウェア バージョンを基に CIM をアップグレードします。一般に、[ファームウェアのアップグレード] ページを使用してデバイスのファームウェアをアップグレードする場合、すべての CIM がアップグレードされます。

注: このページでは、D2CIM-VUSB と D2CIM-DVUSB のみをアップグレードできます。

▶ LX のメモリを使用して CIM をアップグレードするには、以下の手順に従います。

1. [保守] メニューの [CIM ファームウェアのアップグレード] をクリックします。[CIM のアップグレード] ページが開きます。

   [ポート]、[名前]、[タイプ]、[現在の CIM バージョン]、[アップグレード先の CIM バージョン] の各列に情報が表示されるので、各 CIM を簡単に識別できます。
2. アップグレードしたい各 CIM の [選択] チェック ボックスをオンにします。
3. [アップグレード] をクリックします。アップグレードしてもよいかどうかを確認するダイアログ ボックスが開きます。
4. [OK] をクリックしてアップグレード処理を続行します。アップグレード処理中は、進行状況バーが表示されます。アップグレード処理には、CIM ごとに最長で約 2 分かかります。

ファームウェアのアップグレード

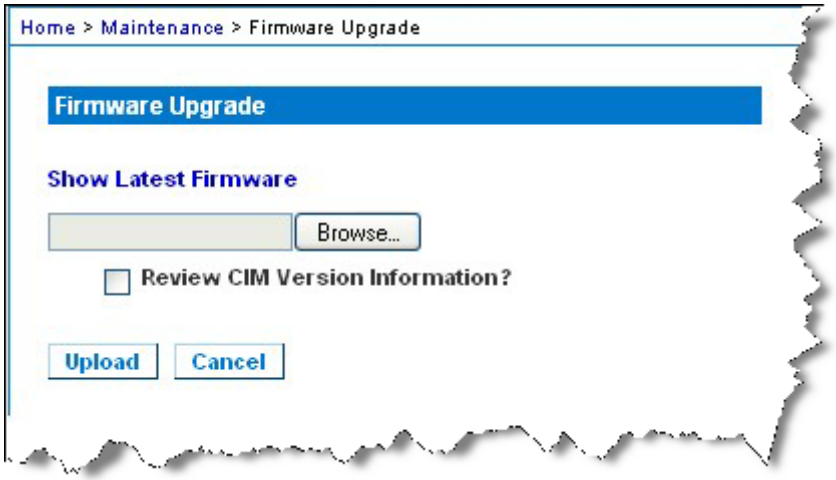
[ファームウェアのアップグレード] ページを使用して、LX および接続するすべての CIM のファームウェアをアップグレードします。このページは、LX リモート コンソールでのみ使用できます。

重要: アップグレード処理中に、LX の電源を切断したり CIM を取り外したりしないでください。LX または CIM が損傷するおそれがあります。

LX をアップグレードするには

1. *Raritan の Web サイト http://www.raritan.com* の [ファームウェアのアップグレード] ページで、適切な Raritan ファームウェア配布ファイル（.rfp ファイル）を探してダウンロードします。
2. そのファイルを解凍します。アップグレードを実行する前に、解凍したファイルに記載されている指示をすべてお読みください。

   注: アップグレードを実行する前に、そのファームウェア配布ファイルをローカル PC にコピーしておいてください。また、そのファームウェア配布ファイルをネットワーク ドライブからロードしないでください。
3. [保守] メニューの [ファームウェアのアップグレード] をクリックします。[ファームウェアのアップグレード] ページが開きます。



4. [参照] をクリックし、ファームウェア配布ファイルを解凍したフォルダに移動します。
5. 使用している CIM のバージョン情報を表示したい場合、[CIM のバージョン情報を確認する] チェック ボックスをオンにします。
6. [ファームウェアのアップグレード] ページの [アップロード] をクリックします。アップグレードとバージョン番号に関する情報が、確認のために表示されます。CIM 情報を表示するよう指定した場合は、その情報も表示されます。

注: この時点で接続していたユーザはログオフされ、新たにログオンしようとしたユーザはブロックされます。

7. [アップグレード] をクリックします。アップグレード処理が完了するまで待機します。アップグレード処理中は、ステータス情報および進行状況バーが表示されます。アップグレード処理が完了すると、LX が再起動します。再起動が完了するとビープ音が 1 回鳴ります。

指示に従ってブラウザを終了し、約 5 分待ってから再度 LX にログオンします。

Multi-Platform Client を使用してデバイスのファームウェアをアップグレードする手順については、『KVM and Serial Access Client Guide』の「Upgrading Device Firmware」を参照してください。

注: モデムを介してファームウェアをアップグレードすることはできません。

アップグレード履歴

LX および接続されている CIM に対して実行されたアップグレード処理に関する情報を表示できます。

▶ **アップグレード履歴を表示するには、以下の手順に従います。**

- [保守] メニューの [アップグレード履歴] をクリックします。[アップグレード履歴] ページが開きます。

実行された LX アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。CIM に関する情報を表示するには、[CIM] 列の [表示] リンクをクリックします。表示される CIM 情報は次のとおりです。

- [タイプ]: CIM のタイプ。
- [ポート]: CIM が接続されているポート。
- [ユーザ]: アップグレード処理を実行したユーザ。
- [IP]: IP アドレス。
- [開始日時]: アップグレード処理の開始日時。
- [終了日時]: アップグレード処理の終了日時。
- [前のバージョン]: アップグレード前の CIM ファームウェア バージョン。
- [アップグレード バージョン]: 現在の CIM ファームウェア バージョン。
- [CIM]: アップグレードされた CIM。
- [結果]: アップグレード処理の結果 (成功または失敗)。

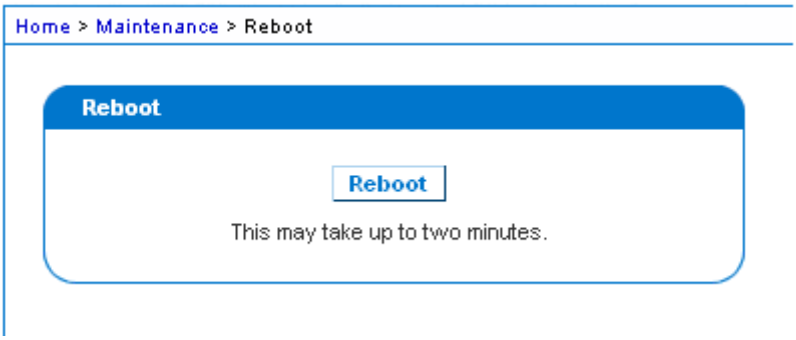
LX の再起動

[Reboot]（再起動）ページでは、LX を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

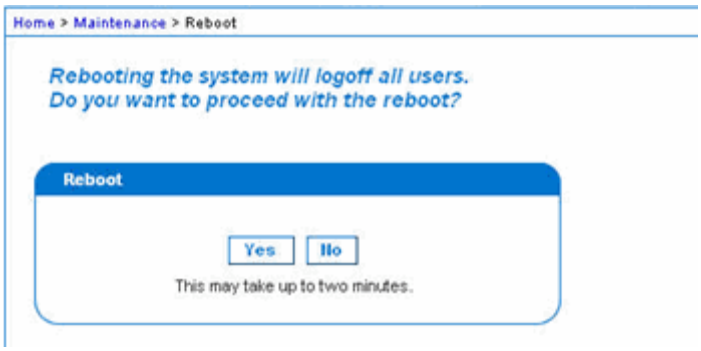
重要: すべての KVM 接続およびシリアル接続が切断され、また、すべてのユーザがログオフされます。

LX を再起動するには

1. [Maintenance]（保守）メニューの [Reboot]（再起動）をクリックします。[Reboot]（再起動）ページが開きます。



2. [Reboot]（再起動）をクリックします。再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes]（はい）をクリックし、再起動処理を続行します。



Ch 9 診断

この章の内容

[ネットワーク インタフェース] ページ

LX では、ネットワーク インタフェースのステータス情報を確認できます。

▶ ネットワーク インタフェースに関する情報を表示するには、以下の手順に従います。

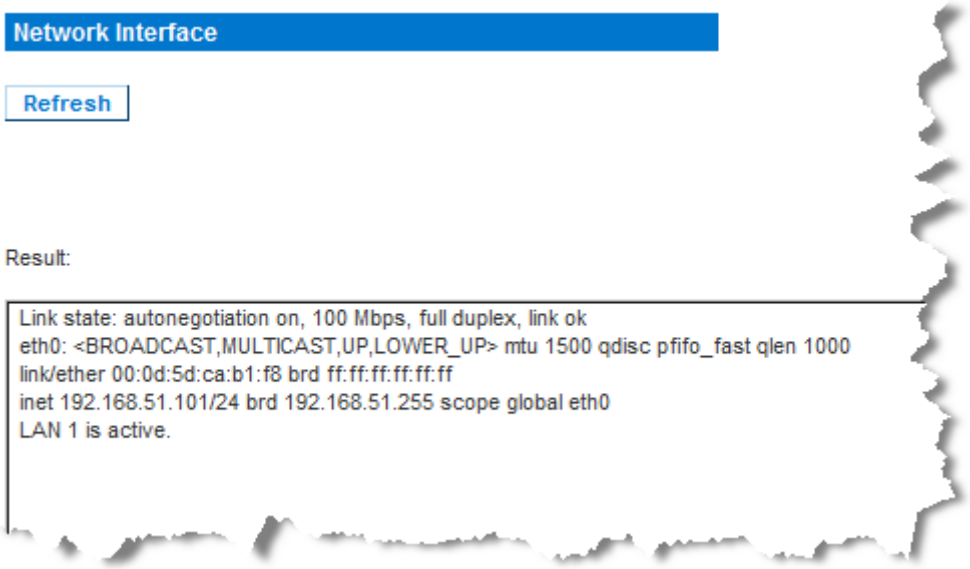
- [診断] メニューの [ネットワーク インタフェース] をクリックします。[ネットワーク インタフェース] ページが開きます。

表示される情報は次のとおりです。

- Ethernet インタフェースが稼動しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

▶ これらの情報を更新するには、以下の手順に従います。

- [更新] をクリックします。



[Network Statistics] (ネットワーク統計) ページ

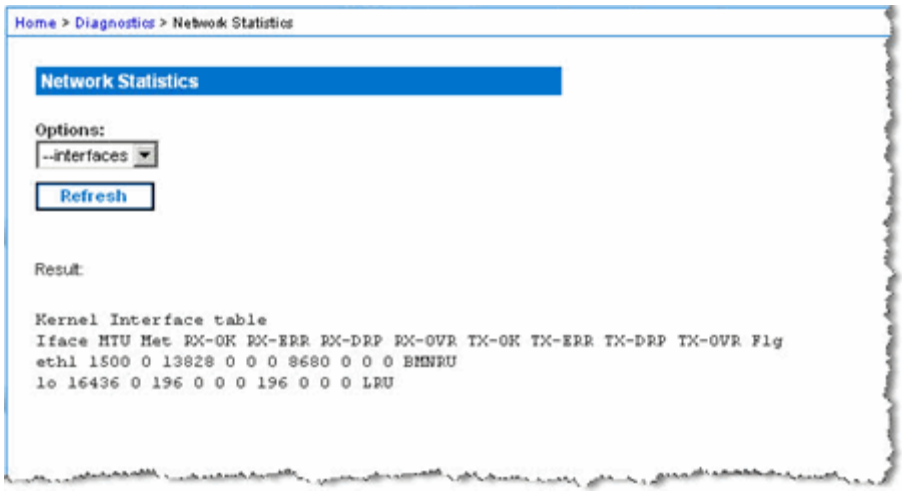
LX では、ネットワーク インタフェースに関する統計情報を表示できます。

▶ ネットワーク インタフェースに関する統計情報を表示するには

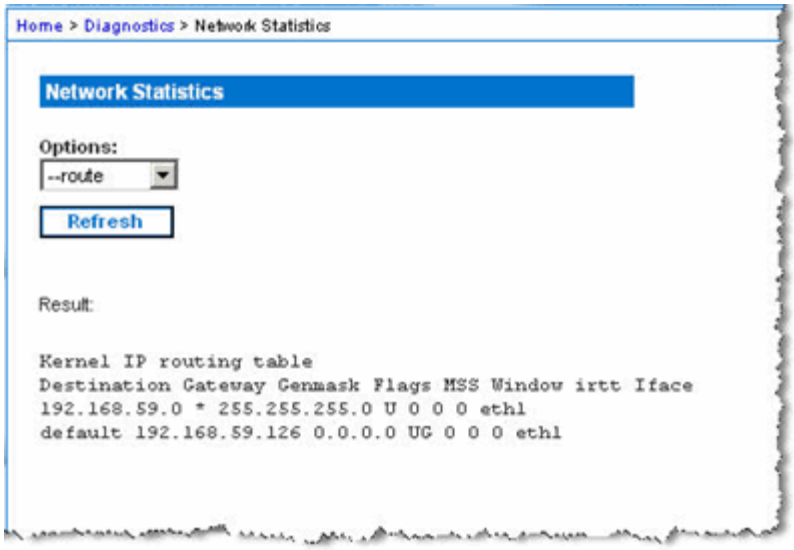
1. [Diagnostics] (診断) メニューの [Network Statistics] (ネットワーク統計) をクリックします。[Network Statistics] (ネットワーク統計) ページが開きます。

2. [Options] (オプション) ボックスの一覧で値を選択します。
   - [Statistics] (統計): 次に示すような情報が表示されます。

   - [Interfaces] (インタフェース): 次に示すような情報が表示されます。



- [Route] (経路): 次に示すような情報が表示されます。



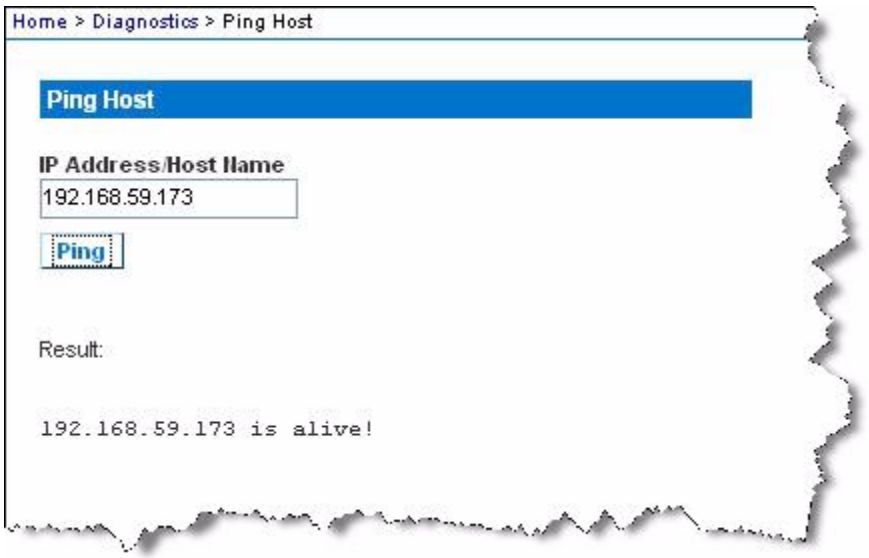
3. [Refresh] (更新) をクリックします。[Options] (オプション) ボックスの一覧で選択した値に応じた情報が、[Result] (結果) フィールドに表示されます。

[ホストに ping する] ページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続可能であるかどうかをテストするためのネットワーク コマンドです。[Ping Host] (ホストに ping する) ページでは、ターゲット サーバまたは別の LX がアクセス可能であるかどうかを調べることができます。

ホストに ping するには

1. [Diagnostics] (診断) メニューの [Ping Host] (ホストに ping する) をクリックします。[Ping Host] (ホストに ping する) ページが開きます。



2. [IP Address/Host Name] (IP アドレス/ホスト名) ボックスに IP アドレスまたはホスト名を入力します。

   注: ホスト名は 232 文字以内で指定してください。

3. [Ping] (ping) をクリックします。ping の実行結果が [Result] (結果) フィールドに表示されます。

[Trace Route to Host] (ホストへの経路をトレースする) ページ

traceroute は、指定したホスト名または IP アドレスへの経路を調べるためのネットワーク コマンドです。

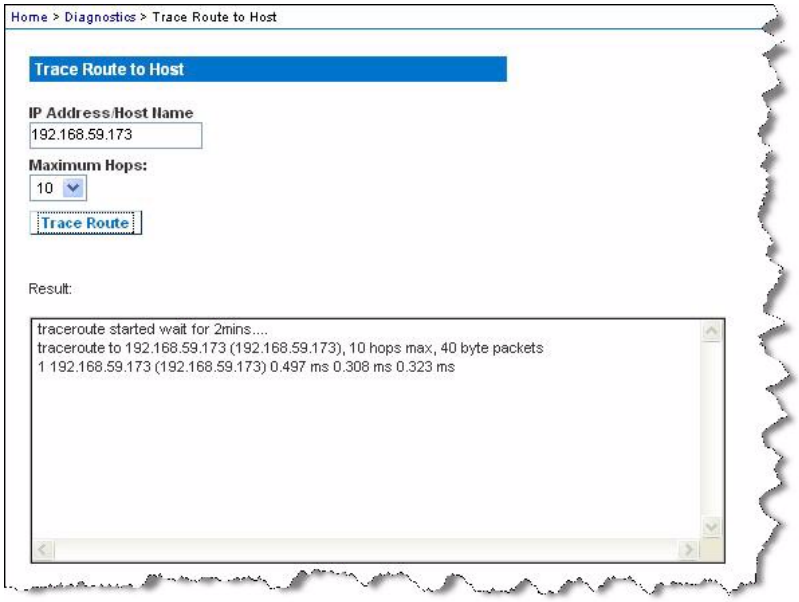
ホストまでの経路をトレースするには

1. [Diagnostics] (診断) メニューの [Trace Route to Host] (ホストへの経路をトレースする) をクリックします。[Trace Route to Host] (ホストへの経路をトレースする) ページが開きます。

2. [IP Address/Host Name] (IP アドレス/ホスト名) ボックスに IP アドレスまたはホスト名を入力します。

   注: ホスト名は 232 文字以内で指定してください。

3. [Maximum Hops] (最大ホップ数) ボックスの一覧で最大ホップ数を選択します (5 刻みで 5 ～ 50)。
4. [Trace Route] (経路をトレースする) をクリックします。traceroute コマンドが、指定したホスト名または IP アドレスに対して、指定した最大ホップ数以内で実行されます。traceroute コマンドの実行結果が [Result] (結果) フィールドに表示されます。



LX 診断

注: これは、Raritan フィールド エンジニアが使用するためのページです。Raritan のテクニカル サポート部門から指示された場合に限り、ユーザも使用できます。

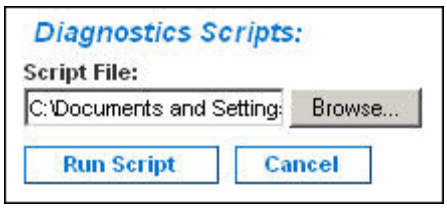
[LX 診断] ページでは、診断情報を LX からクライアント コンピュータにダウンロードできます。このページでは、次の 2 種類の処理を行うことができます。

- 重大エラー デバッグ セッション中に、Raritan のテクニカル サポート部門から提供された特別な診断スクリプトを実行する。このスクリプトは、LX にアップロードされ、実行されます。このスクリプトの実行が完了した後、[ファイルに保存] 機能を使用して診断メッセージをダウンロードできます。
- 診断メッセージのスナップショットに対するデバイス診断ログを、LX からクライアント コンピュータにダウンロードする。このダウンロードされたデバイス診断ログは暗号化ファイルであり、Raritan のテクニカル サポート部門に送信されます。このファイルを解析できるのは Raritan だけです。

注: このページを開くことができるのは、管理者権限を持つユーザだけです。

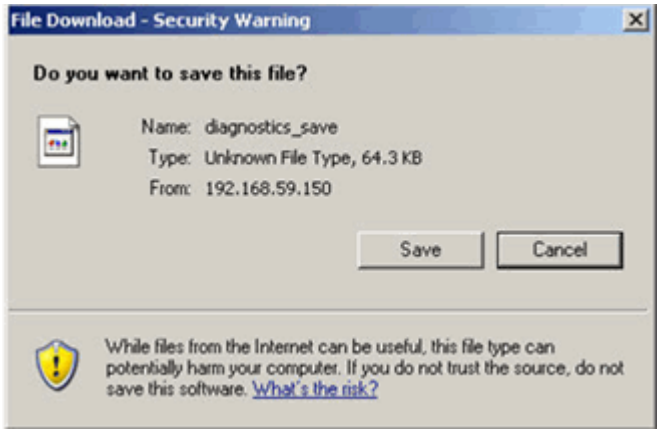
▶ LX のシステム診断を実行するには、以下の手順に従います。

1. [診断] メニューの [LX 診断] をクリックします。[LX 診断] ページが開きます。
2. Raritan のテクニカル サポート部門から電子メールで受け取った診断スクリプト ファイルを実行するため、次の手順を実行します。
   a. Raritan から提供されている診断スクリプト ファイルを入手します。圧縮されている場合は解凍します。
   b. [参照] をクリックします。[ファイルを選択] ダイアログ ボックスが開きます。
   c. 診断スクリプト ファイルを探して選択します。
   d. [開く] をクリックします。診断スクリプト ファイルの名前が [スクリプト ファイル] ボックスに表示されます。



   e. [スクリプトを実行] をクリックします。この診断スクリプト ファイルを Raritan のテクニカル サポート部門に送信します。

3. 診断ファイルを作成して Raritan のテクニカル サポート部門に送信するため、次の手順を実行します。
   a. [ファイルに保存] をクリックします。[ファイルのダウンロード] ダイアログ ボックスが開きます。



   b. [保存] をクリックします。[名前を付けて保存] ダイアログ ボックスが開きます。
   c. 保存先フォルダに移動し、[保存] をクリックします。
   d. Raritan のテクニカル サポート部門の指示に従って、このファイルを E メールで送信します。

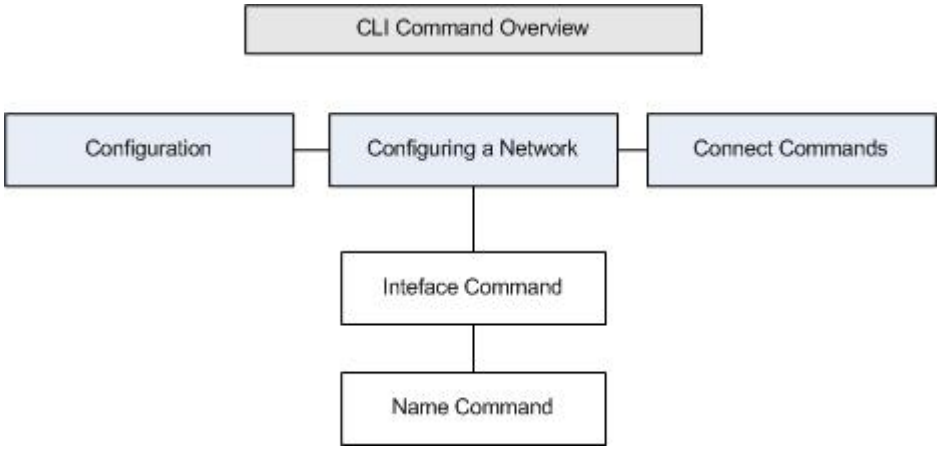
Ch 10 コマンド ライン インタフェース (CLI)

この章の内容

概要

LX のネットワーク インタフェースを設定する権限や診断処理を実行する権限を持っている場合、コマンド ライン インタフェース (CLI) を使用してそれらの処理を実行できます。

次の図に CLI コマンドの概要を示します。コマンドの一覧については、「*CLI コマンド 『187*p. 』」を参照してください。この一覧には、各コマンドの説明、および、各コマンドの記述例が書かれている項へのリンクがあります。



top、history、log off、quit、show、help の各コマンドは、この図のどの CLI レベルからでも使用できます。

CLI を使用しての LX へのアクセス

次の方法のいずれかを使用して、LX にアクセスします。

- IP 接続を介した SSH (Secure Shell)

複数の SSH クライアントを使用可能で、次の場所から取得できます。

- Putty: *http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/*参照
- ssh.com の SSH クライアント: *www.ssh.com http://www.ssh.com* 参照
- Applet SSH Client: *www.netspace.org/ssh http://www.netspace.org/ssh* 参照
- OpenSSH Client: *www.openssh.org http://www.openssh.org* 参照

LX への SSH 接続

SSHv2 をサポートする Secure Shell (SSH) クライアントを使用して、LX に接続します。[Devices Services] (デバイス サービス) ページで SSH 接続を有効にしておく必要があります。

注: セキュリティ上の理由により、SSHv1 接続は LX でサポートされていません。

Windows PC から SSH で接続する

▶ **Windows® PC から SSH セッションを開くには**

1. SSH クライアント ソフトウェアを起動します。
2. LX サーバの IP アドレスを入力します (例: 「192.168.0.192」)。
3. SSH を選択します。SSH では、デフォルトの設定ポート 22 が使用されます。
4. [Open] (開く) をクリックします。

`login as:` (ログイン) プロンプトが表示されます。

「*ログイン 『184*p. 』」を参照してください。

UNIX/Linux ワークステーションから SSH で接続する

▶ **UNIX®/Linux® ワークステーションから SSH セッションを開き、ユーザ admin としてログオンするため、次のコマンドを入力します。**

```
ssh -l admin 192.168.30.222
```

パスワードの入力を求めるプロンプトが表示されます。

「*ログイン 『184*p. 』」を参照してください。

ログイン

▶ **ログインするには、次のようにユーザ名 admin を入力します。**

1. admin としてログインします。
2. パスワードの入力を求めるプロンプトが表示されます。デフォルトパスワード（「raritan」）を入力します。

   歓迎メッセージが表示されます。これで、管理者としてログオンしたことになります。

次項「*CLI の画面操作 『184p. 』*」の内容を確認した後、初期設定処理を実行します。

CLI の画面操作

CLI を使用する前に、CLI の画面操作と構文について理解しておくことが重要です。また、CLI の使用を簡素化するキー入力の組み合わせについても、理解しておく必要があります。

コマンドのオート コンプリート

CLI にはオート コンプリート機能（コマンドの一部を入力すると、残りの部分が自動入力される機能）が備わっています。先頭の数文字を入力した後、Tab キーを押します。入力した文字列で始まるコマンドの候補が 1 つしかない場合、オート コンプリート機能によって残りの部分が自動入力されます。

- 入力した文字列で始まるコマンドの候補が見つからない場合、そのレベルに対する有効な入力候補が表示されます。
- 入力した文字列で始まるコマンドの候補が複数個見つかった場合、すべての入力候補が表示されます。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、Tab キーを押してコマンドを自動入力します。

CLI 構文: ヒントとショートカット キー

ヒント

- コマンドは、アルファベット順に表示されています。
- コマンドでは、大文字と小文字は区別されません。
- パラメータ名は、アンダスコアを含まない 1 つの単語です。
- コマンドに対して引数を指定しない場合、そのコマンドに対する現在の設定値が指定されていると見なされます。
- コマンドの後ろに疑問符 (?) を指定した場合、そのコマンドに対するヘルプが表示されます。
- 縦線 (|) は、任意指定または必須指定のキーワードまたは引数における、選択肢を意味します。

ショートカット

- 末尾のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、Backspace キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- コマンドを実行するには、Enter キーを押します。
- コマンドの入力中に残りの部分を自動入力するには、Tab キーを押します。たとえば、Admin Port > プロンプトで Conf と入力した後に Tab キーを押すと、`Admin Port > Config >` プロンプトが表示されます。

すべての CLI レベルで使用できるコマンド

次の表に、すべての CLI レベルで使用できるコマンドを示します。これらのコマンドは、CLI の画面操作にも役立ちます。

コマンド	説明
top	CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
history	LX の CLI で入力した最後の 200 個のコマンドが表示されます。
help	CLI 構文の概要が表示されます。
quit	1 レベル上に戻ります。
logout	ユーザ セッションが終了し、ユーザがログオフされます。

CLI を使用した初期設定

注: この項で説明する、CLI を使用した手順の実行は任意です。LX ローカル コンソールで同じ設定作業を実行できるからです。詳細については、「最初に行う作業 『13p. の "入門" 参照 』」を参照してください。

LX は、デフォルト値に設定された状態で工場から出荷されます。初めて電源を入れて接続を行う際、次のとおりに基本パラメータ値を設定し、ネットワーク上から LX に安全にアクセスできるようにする必要があります。

1. 管理者パスワードを再設定します。LX は、すべてのデバイスに同じデフォルト パスワードが設定された状態で出荷されます。したがって、セキュリティ侵害を回避するため、管理者パスワードをデフォルトの raritan から変更する必要があります。新しいパスワードは、LX の管理者になるユーザが決めます。
2. IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値を設定し、リモート アクセスできるようにします。

パラメータ値を設定する

パラメータ値を設定するには、管理者権限でログオンする必要があります。CLI 階層の最上位である username > プロンプトが表示されます。初期設定を行うため、admin と入力します。top コマンドを入力し、最上位レベルに戻ります。

注: admin 以外のユーザ名でログオンした場合、admin の代わりにそのユーザ名が表示されます。

ネットワーク パラメータの設定

ネットワーク パラメータ値を設定するには、interface コマンドを使用します。

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

このコマンドが受け付けられると、LX との接続が自動切断されます。新たに設定した IP アドレス、および、「パラメータ値を設定する」で作成したユーザ名とパスワードを使用して、LX に再接続します。

重要: パスワードを忘れてしまった場合は、LX の背面にあるリセット ボタンを押し、出荷時設定に戻す必要があります。この場合、初期設定作業を再度実行する必要があります。

これで LX の基本情報が設定されたので、SSH またはグラフィカル ユーザ インタフェース (GUI) を使用してリモート アクセスすることや、ローカル シリアル ポートを使用してローカル アクセスすることができます。管理者は、ユーザ、グループ、サービス、セキュリティ、およびシリアル ポートを設定する必要があります。シリアル ポートは、シリアル ターゲットを LX に接続するためのポートです。

CLI プロンプト

CLI プロンプトは、現在のコマンド レベルを意味しています。プロンプトのルート部分はログオン名です。端末エミュレーション ソフトウェアを使用して管理用シリアル ポートに直接接続している場合、コマンドのルート部分は Admin Port になります。

```
admin >
```

SSH で接続している場合、コマンドのルート部分は admin になります。

```
admin > config > network >
```

0

CLI コマンド

- `admin > help` と入力した場合に使用できるコマンドは、次のとおりです。

コマンド	説明
config	config サブメニューに切り替えます。
diagnostics	diag サブメニューに切り替えます。
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
listports	使用可能なポートを一覧表示します。
logout	現在の CLI セッションを終了し、ログオフします。
top	ルート メニューに戻ります。
userlist	アクティブなユーザ セッションを一覧表示します。

- 「admin > config > network」と入力します。

コマンド	説明
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
interface	ネットワーク パラメータ値を取得および設定します。
ipv6_interface	IPv6 のネットワーク パラメータ値を取得および設定します。
logout	現在の CLI セッションを終了し、ログオフします。
name	デバイス名を設定します。
quit	前のメニューに戻ります。
stop	ルート メニューに戻ります。

セキュリティ上の問題

コンソール サーバにおけるセキュリティを確保する際に検討すべき点は、次のとおりです。

- 運用担当者用コンソールと LX との間で送受信されるデータ トラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- セキュリティ プロファイルを設定する。

LX にはこの 3 つの機能がすべて備わっています。ただし、設定作業は運用開始前に済ませておく必要があります。

LX コンソール サーバ設定用コマンドを使用する

注: SSH 接続とローカル ポート接続では、CLI コマンドは同じです。

network コマンドは、Configuration メニューで使用できます。

ネットワークを設定する

network メニューのコマンドを使用して、LX のネットワーク インタフェースを設定します。

コマンド	説明
interface	LX のネットワーク インタフェースを設定します。
name	ネットワーク名を設定します。
ipv6	IPv6 のネットワーク パラメータ値を取得および設定します。

interface コマンド

interface コマンドを使用して、LX のネットワーク インタフェースを設定します。**interface コマンドの構文は次のとおりです。**

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <mode>]
Ethernet パラメータ値を設定/取得します。
ipauto <none|dhcp>: IP アドレスを自動設定するかどうか (none/dhcp)。
ip <ipaddress>: IP アドレス。
mask <subnetmask>: サブネット マスク。
gw <ipaddress>: デフォルト ゲートウェイ。
mode <mode>: Ethernet モードを設定 (auto/10hdx/10fdx/100hdx/100fdx/1000fdx)。
```

interface コマンドの例

次のコマンドを実行すると、インタフェース番号 1 が有効になり、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値が設定され、Ethernet モードが自動検出に設定されます。

```
Admin > Config > Network > interface ipauto none ip 192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode auto
```

name コマンド

name コマンドを使用して、ネットワーク名を設定します。name コマンドの構文は次のとおりです。

```
name [devicename <devicename>] [hostname <hostname>]
```

デバイス名の設定

```
devicename <devicename>: デバイス名。
hostname <hostname>: 優先ホスト名 (DHCP 使用時のみ)。
```

name コマンドの例

次のコマンドを実行すると、ネットワーク名が設定されます。

```
Admin > Config > Network > name devicename My-KSX2
```

ipv6 コマンド

ipv6 コマンドを使用して、IPv6 関連のネットワーク パラメータ値の設定と取得を行います。

Ch 11 LX ローカル コンソール

この章の内容

概要

LX のローカル ポートにコンピュータを接続して LX ローカル コンソールを使用することにより、設置場所で管理作業を行うことができます。この LX ローカル コンソールの特徴は、ブラウザを使用する、という点であり、サーバをすばやく切り替えることができます。LX ローカル コンソールでは、LX に接続されているサーバのキーボード ポート、マウス ポート、およびビデオ ポートに直接接続している場合と同等のパフォーマンスが得られます。また、LX ローカル コンソールには、LX リモート コンソールと同等の管理機能が備わっています。

ユーザが同時接続可能

LX ローカル コンソールを使用する場合、接続されている各 KVM ターゲット サーバへの独立したアクセス パスが設定されます。つまり、LX ローカル コンソールを使用している最中でも、他ユーザがネットワーク経由で LX に同時接続できます。また、リモート ユーザが LX に接続している最中でも、LX ローカル コンソールを使用してラックからサーバに同時接続できます。

LX ローカル コンソール インタフェース: LX デバイス

サーバ ラックに設置した LX の場合は、LX ローカル コンソールを介して、標準 KVM 管理を行います。LX ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。

LX ローカル コンソールと LX リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

[LX Local Console Factory Reset] (LX ローカル コンソール ファクトリ リセット) オプションは、LX ローカル コンソールには用意されていますが、LX リモート コンソールには用意されていません。

セキュリティと認証

LX ローカル コンソールを使用するには、まず有効なユーザ名とパスワードで認証を受ける必要があります。LX には認証機能とセキュリティ機能が備わっています。これらの機能は、ネットワークから接続するユーザとローカル ポートから接続するユーザの両方に対して有効です。ユーザは、どちらの方法で接続する場合でも、アクセス権限を持っているサーバにしかアクセスできません。サーバ アクセスとセキュリティに関する設定情報を指定する手順については、「*ユーザ管理 『104*p. の *"[User Management] (ユーザ管理)"* 参照 』」を参照してください。

LX が外部認証サービス (LDAP/LDAPS、RADIUS、または Active Directory) を使用するように設定されている場合、ユーザが LX ローカル コンソールを使用して接続する際でも、外部認証サービスによって認証が行われます。

注: LX ローカル コンソールを使用して接続しようとするユーザに対して認証を行わないように、設定することもできます。ただし、この方法は安全な環境でのみ使用することを推奨します。

▶ LX ローカル コンソールを使用するには

1. キーボード、マウス、およびモニタを、LX の背面にあるローカル ポートに接続します。
2. LX を起動します。LX ローカル コンソール画面が表示されます。

サポートされている画面解像度 - ローカル コンソール

各ターゲット サーバの画面解像度とリフレッシュ レートが LX でサポートされているかどうか、および、映像信号がノンインタレース方式であるかどうかを確認してください。

LX ローカル コンソールは次の解像度に対応しており、さまざまなモニタで適切に表示されます。

- 800 x 600
- 1024 x 768
- 1280 x 1024

これらの各解像度について、60 Hz と 75 Hz の垂直走査周波数がサポートされています。

画面解像度とケーブル長は、マウスを同期させるうえで重要な要素です。「*ターゲット サーバとの接続距離および画面解像度* 『*210*p. 』」を参照してください。

[ポート アクセス] ページ (ローカル コンソール サーバ ディスプレイ)

LX ローカル コンソールにログオンすると、[ポート アクセス] ページが開きます。このページには、LX のポート、各ポートに接続されている KVM ターゲット サーバ、および各ターゲット サーバのステータスと稼動状態が一覧表示されます。

ティアー接続構成にしており、ベース LX デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、 カスケード接続デバイスは、[ポート アクセス] ページでカスケード接続デバイス名の左にある展開矢印アイコン ▶ をクリックすると表示されます。カスケード接続の詳細については、「*カスケード接続の設定および有効化* 『*135*p. 』」を参照してください。

▶ [ポート アクセス] ページを使用するには、以下の手順に従います。

1. LX ローカル コンソールにログインします。
2. [ポート アクセス] タブをクリックします。[ポート アクセス] ページが開きます。

   KVM ターゲット サーバは当初ポート番号順に並んでいますが、列のいずれかを基準に表示順を変更できます。

   - [Port Number] (ポート番号) - 1 から LX デバイスで使用できるポートの合計数までの番号が振られています。
   - [ポート名]: LX ポートの名前です。最初は、「Dominion-LX-Port#」に設定されていますが、わかりやすい名前に変更できます。[ポート名] のリンクをクリックすると、[ポート アクション] メニューが表示されます。

注: ポート (CIM) 名にアポストロフィ (″ ′ ″) を使用することはできません。

- [タイプ]: サーバまたは CIM のタイプです。
- [ステータス]: 標準サーバのステータスは [アップ] または [ダウン] のどちらかです。
- [可用性]: サーバの可用性です。

3. アクセスするターゲット サーバのポート名をクリックします。[ポート アクション] メニューが表示されます。使用可能なメニュー オプションの詳細については、「[ポート アクション] メニュー」を参照してください。
4. [ポート アクション] メニューから、目的のメニュー コマンドを選択します。

表示順を変更したり同じページにさらにポートを表示したりするには、以下の手順に従います。

1. 並べ替えで基準にする列の見出しをクリックします。その列に基づいて KVM ターゲット サーバのリストが並べ替えられます。
2. [1 ページ当たりの行] に、ページに表示するポート数を入力し、[設定] をクリックします。

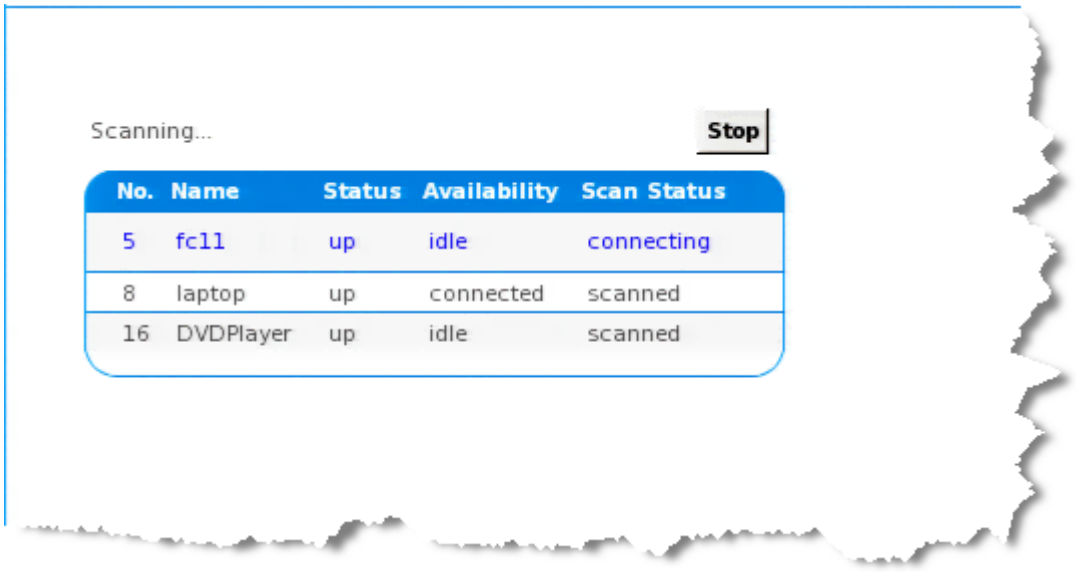
ターゲット サーバにアクセスする

ターゲット サーバにアクセスするには

1. アクセスしたいターゲット サーバのポート名をクリックします。ポート アクション メニューが開きます。
2. ポート アクション メニューの [Connect] (接続) をクリックします。そのターゲット サーバの画面に切り替わります。

ポートのスキャン - ローカル コンソール

LX のスキャン機能は、ローカル コンソールでサポートされています。スキャンで見つかったターゲットは、1 つずつ［スキャン］ページに表示されます。これは、リモート コンソールのポート スライド ショーとは異なります。各ターゲットがページにデフォルトで 10 秒間表示されるので、ターゲットを確認して接続できます。表示されているターゲットに接続するには、ローカル ポートの ConnectKey シーケンスを使用します。また、そのターゲットから切断するには、DisconnectKey のシーケンスを使用します。



▶ ターゲットをスキャンするには、以下の手順に従います。

1. ローカル コンソールで、［ポート アクセス］ページの［スキャン設定］タブをクリックします。
2. 各ターゲットの横にあるチェックボックスをオンにしてスキャン対象に含めるターゲットを個別に選択するか、ターゲット列の上部にあるチェックボックスをオンにしてすべてのターゲットを選択します。
3. アップ ステータスのターゲットだけをスキャンに含める場合は、［アップのみ］チェックボックスをオンのままにします。アップかダウンかに関係なくすべてのターゲットを含める場合は、このチェックボックスをオフにします。
4. ［スキャン］をクリックしてスキャンを開始します。［ポート スキャン］ウィンドウが開きます。ターゲットが見つかるたびに、それがウィンドウに表示されます。
5. ターゲットが表示されたら、ConnectKey シーケンスを使用してそれに接続します。
6. ［スキャンの停止］をクリックしてスキャンを停止します。

スキャン オプションの使用

ターゲットのスキャン中は、次のオプションを使用できます。これらのすべてのオプションは、[Expand]（展開）/[Collapse]（折りたたみ）アイコンを除き、[Port Scan]（ポート スキャン）ビューアの左上の [Options]（オプション）メニューから選択します。ウィンドウを閉じると、オプションはデフォルトに戻ります。

サムネイルの表示または非表示

- ウィンドウの左上の [Expand]（展開）/[Collapse]（折りたたみ）アイコン  を使用して、サムネイルを表示または非表示にします。デフォルト表示では展開されています。

サムネイル スライド ショーの一時停止

- [Options]（オプション）の [Pause]（一時停止）を選択すると、あるターゲットから次のターゲットへのサムネイルのローテーションが一時停止します。サムネイルのローテーションはデフォルト設定です。

サムネイル スライド ショーの再開

- [Options]（オプション）の [Resume]（再開）を選択すると、サムネイルのローテーションが再開されます。

[Port Scan] (ポート スキャン) ビューアのサムネイルのサイズ変更

- サムネイルを拡大するには、[Options]（オプション）、[Size]（サイズ）、[360x240] の順に選択します。
- サムネイルを最小化するには、[Options]（オプション）、[Size]（サイズ）、[160x120] の順に選択します。これはデフォルトのサムネイル サイズです。

[Port Scan] (ポート スキャン) ビューアの表示方向の変更

- [Options]（オプション）、[Split Orientation]（分割方向）、[Horizontal]（横）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの下部に沿って表示されます。
- [Options]（オプション）、[Split Orientation]（分割方向）、[Vertical]（縦）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの右側に沿って表示されます。これがデフォルト表示です。

ホット キーと接続キー

LX ローカル コンソールの画面は、現在アクセスしているターゲット サーバの画面に完全に置き換えられます。ターゲット サーバから切断し、ローカル コンソールの画面に戻るには、ホット キーを使用します。接続キーは、ターゲット サーバに接続したり、ターゲット サーバを切り替えたりする際に使用します。

ターゲット サーバの画面が表示されているときにホットキーを使用することにより、LX ローカル コンソールの画面をすばやく開くことができます。デフォルトでは、Scroll Lock キーをすばやく 2 回押します。別のキー シーケンスをホットキーとして指定することもできます。指定するには、[ローカル ポート設定] ページを使用します。詳細については、「LX ローカル コンソールのローカル ポートの設定」を参照してください。

接続キーの例

標準型サーバの場合 接続キーを押したときのアクション	キー シーケンスの例
LX ローカル コンソールからポートに接続する	LX ローカル コンソールからポート 5 に接続するには • 左 Alt キーを押す → 5 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 からポート 11 に切り替えるには • 左 Alt キーを押す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、LX ローカル コンソールの画面に戻る	ポート 11 から切断し、LX ローカル コンソールの画面（ターゲット サーバに接続する時に開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す

Sun サーバへのアクセス時に使用できる特別なキー組み合わせ

ローカル ポートでは、Sun Microsystems™ サーバの特別なキーに対して、次のキー組み合わせが機能します。これらの特別なキー組み合わせは、Sun ターゲット サーバに接続しているときに使用できます。

Sun サーバのキー	ローカル ポートにおけるキー組み合わせ
Again	Ctrl+ Alt +F2
Props	Ctrl+ Alt +F3
Undo	Ctrl+ Alt +F4
Stop A	Break a
Front	Ctrl+ Alt +F5
Copy	Ctrl+ Alt +F6
Open	Ctrl+ Alt +F7
Find	Ctrl+ Alt +F9
Cut	Ctrl+ Alt +F10
Paste	Ctrl+ Alt +F8
Mute	Ctrl+ Alt +F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	キー組み合わせなし
電力	キー組み合わせなし

LX ローカル コンソールの画面に切り替える

重要: LX ローカル コンソールのデフォルトのホットキーは、Scroll Lock キーをすばやく 2 回押すことです。このキー組み合わせを変更するには、[Local Port Settings] (ローカル ポート設定) ページを使用します。「ローカル コンソールからの LX ローカル ポートの設定」を参照してください。

▶ ターゲット サーバの画面から LX ローカル コンソールの画面に戻るには

- ホットキーを押します (デフォルトでは Scroll Lock キーをすばやく 2 回押す)。ターゲット サーバの画面から LX ローカル コンソールの画面に切り替わります。

ローカル ポートの管理

LX を管理するには、LX ローカル コンソールまたは LX リモート コンソールを使用します。LX ローカル コンソールには次のページもあります。

- [Factory Reset] (出荷時設定にリセット)
- [Local Port Settings] (ローカル ポート設定)(LX リモート コンソールにもある)

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

LX ローカル コンソールのローカル ポートの設定

[Local Port Settings] (ローカル ポート設定) ページでは、LX ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

▶ ローカル ポートに関する設定値をカスタマイズするには

注: [Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. 標準ローカル ポートを有効にするには、[標準ローカル ポートを有効にする] チェック ボックスをオンにします。無効にするにはチェックボックスをオフにします。デフォルトでは、標準ローカル ポートは有効になっていますが、必要に応じて無効にすることができます。カスケード接続機能を利用する場合、この機能は無効になります。両方の機能を同時に利用することができないからです。

3. カスケード接続機能を利用する場合、[ローカル ポート デバイスのカスケード接続を有効にする] チェック ボックスをオンにし、[カスケード接続秘密ワード] フィールドにカスケード接続秘密ワードを入力します。カスケード接続を設定するには、[デバイス サービス] ページでベース デバイスを設定する必要があります。カスケード接続の詳細については、「*カスケード接続の設定および有効化*『*135*p. 』」を参照してください。
4. 必要な場合は、[ローカル ポート スキャン モード] 設定をカスタマイズします。これらの設定は、[ポート] ページからアクセスされるスキャン設定機能に適用されます。「*ポートのスキャン* 『*48*p. 』」を参照してください。
   - [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
   - [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
5. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)
   - [United Kingdom] (イギリス英語)
   - [French (France)] (フランス語 (フランス))
   - [German (Germany)] (ドイツ語 (ドイツ))
   - [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
   - [Simplified Chinese] (簡体字中国語)
   - [Traditional Chinese] (繁体字中国語)
   - [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
   - [German (Switzerland)] (ドイツ語 (スイス))
   - [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
   - [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
   - [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
   - [Danish (Denmark)] (デンマーク語 (デンマーク))
   - [Belgian (Belgium)] (ベルギー語 (ベルギー))

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

注: トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

6. [Local Port Hotkey](ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに LX ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock](Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock] (Caps Lock キーを 2 回押す)	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。

7. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。その後ホットキーを使用して、そのターゲット サーバの画面から LX ローカル コンソールの画面に戻すことができます。接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー シーケンスの例については、「接続キーの例」を参照してください。
8. [OK] (OK) をクリックします。

LX ローカル コンソールの [出荷時設定にリセット] ページ

注: このページは、LX ローカル コンソールでのみ使用できます。

LX ローカル コンソールでは、さまざまなリセット モードの中から適切なものを選択できます。

*注: 出荷時設定にリセットする前に、監査ログを保存しておくことをお勧めします。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「**監査ログ**『165p. の"[Audit Log](監査ログ)"参照 』」を参照してください。*

▶ 出荷時設定にリセットするには、以下の手順に従います。

1. [保守] メニューの [出荷時設定にリセット] をクリックします。[出荷時設定にリセット] ページが開きます。
2. リセット モードを選択します。選択できるオプションは次のとおりです。
   - [完全リセット]: すべての設定値を削除し、工場出荷時のデフォルト値にリセットします。LX が CC-SG の管理下にある場合は、CC-SG との関連付けが解除されます。このリセット モードではすべての設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
   - [ネットワーク パラメータ値をリセット]: LX のネットワーク パラメータ値を出荷時設定にリセットします。現在設定されているネットワーク パラメータ値を表示するには、[デバイス設定] メニューの [ネットワーク設定] をクリックします。リセットされる設定値は次のとおりです。
     - IP を自動設定するかどうか
     - IP アドレス
     - サブネット マスク
     - ゲートウェイ IP アドレス
     - プライマリ DNS サーバの IP アドレス
     - セカンダリ DNS サーバの IP アドレス
     - 検出ポート
     - 帯域幅制限
     - LAN インタフェースの速度と通信方式 (全二重/半二重)
3. [リセット] をクリックして続行します。すべてのネットワーク設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
4. [OK] をクリックして続行します。リセットが完了すると、LX が自動再起動します。

リセット ボタンを使用して LX をリセットする

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように、ボタンはパネルに埋め込まれています (このボタンを使用するには、先端が尖った道具が必要です)。

リセット ボタンを押したときに実行される処理については、グラフィカル ユーザ インタフェースで定義します。「*暗号化および共有『159p. 』*」を参照してください。

*注: 出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「***監査ログ** *『165p. の「[Audit Log] (監査ログ)」参照 』」を参照してください。*

▶ **デバイスをリセットするには、以下の手順に従います。**

1. LX の電源を切ります。
2. 先端の尖った道具を使用してリセット ボタンを押し続けます。
3. リセット ボタンを押したまま、LX の電源を入れ直します。
4. リセット ボタンを 10 秒間押したままにします。デバイスがリセットされると、短いビープ音が 2 回鳴り、リセットが完了した旨が通知されます。

Ap A 仕様

この章の内容

LX の仕様

Dominion LX モデル	説明	製品寸法 (幅 x 奥行き x 高さ)、出荷重量と電源	環境
DLX-108	経済的で拡張可能な 8 ポート KVM-over-IP スイッチ、1 リモート ユーザ、1 ローカル ユーザ、仮想メディア、単一電源と単一 LAN	11.45″ x 10.63 ″ x1.73″、291mm x 270mm x 44mm 8.82lbs、4.0kg 単一電源 100-240V AC、50 ～ 60Hz、0.5A、30W、25.794kcal/h	使用温度: 0 ～ 40° C (32 ～ 104° F) 湿度: 20 ～ 85% (相対湿度)
DLX-116	経済的で拡張可能な 16 ポート KVM-over-IP スイッチ、1 リモート ユーザ、1 ローカル ユーザ、仮想メディア、単一電源と単一 LAN		
DLX-216	経済的で拡張可能な 16 ポート KVM-over-IP スイッチ、2 リモート ユーザ、1 ローカル ユーザ、仮想メディア、単一電源と単一 LAN		

サポートされているハードウェア	
フォーム ファクタ	1U、ラックマウント対応（ブラケット付属）
ローカル アクセス ポート	ビデオ: HD15(F) VGA、キーボード/マウス: USB(F)、3 USB（背面）
サンプル画面解像度	PC テキストモード: 640 x 350、640 x 480、720 x 400 PC グラフィック モード: 640 x 480、800 x 600、1024 x 768、1152 x 864、1280 x 1024、1440 x 900、1680 x 1050、1600 x 1200、1920 x 1080 Sun ビデオ モード: 1024 x 768、1152 x 864、1152 x 900、1280 x 1024
リモート接続	
ポート	8（DLX-108）または 16（DLX-116、DLX-216）
ユーザ	ローカル ユーザ、1 または 2 リモート ユーザ（モデルによって異なる）
ネットワーク	単一の 10/100/1000 ギガビット Ethernet アクセス、デュアル スタック: IPv4 と IPv6
プロトコル	TCP/IP、HTTP、HTTPS、UDP、RADIUS、SNMP、DHCP、PAP、CHAP
コンピュータ インタフェース モジュール (CIM) と Cat5 ケーブル	
Dominion CIM	USB、デュアル USB、ユニバーサル仮想メディア/ずれないマウス、PS2、Sun、シリアル デバイスで利用可能 寸法（幅 x 奥行き x 高さ）= 1.7″ x 3.5″ x 0.8″、43mm x 90mm x 19mm（デュアル USB）および 1.3″ x 3.0″ x 0.6″、33mm x 76mm x 15mm（その他の DCIM）
Cat5 MCUTP ケーブル	PS/2、USB、Sun の KVM UTP ケーブル: 長さ 0.6m（2 フィート）～ 6m（20 フィート）。仕様: RJ45 <-> HDB-15M、mini-din 6 x 2（PS/2）、USB タイプ A（USB/Sun）
サービスとサポート	
保証*	標準 2 年保証（先出し交換あり）

LED インジケータ

前面パネル LED

- 起動: 青色および赤色 LED が点灯
- 動作時: 青色
- ファームウェア アップグレード: 青色 LED が点滅

背面パネル LED

- 10 Mbps/半二重: 両方の LED が点滅
- 10 Mbps/全二重: 両方の LED が点滅
- 100 Mbps/半二重: 黄色の LED が点滅
- 1 Gbps/全二重: 緑色の LED が点滅

サポートされているオペレーティング システム (クライアント)

Virtual KVM Client (VKC) および Multi-Platform Client (MPC) でサポートされているオペレーティング システム (OS) は、次のとおりです。

クライアント オペレーティング システム	クライアントで仮想メディア (VM) がサポートされているか
Windows 7®	はい
Windows XP®	はい
Windows 2008®	はい
Windows Vista®	はい
Windows 2000® SP4 Server	はい
Windows 2003® Server	はい
Windows 2008® Server	はい
Red Hat® Desktop 5.0	はい
Red Hat Desktop 4.0	はい
openSUSE 10、11	はい
Fedora® 13 および 14	はい
Mac® OS	はい
Solaris™	いいえ
Linux®	はい

Java Runtime Environment (JRE™) プラグインは、32 ビット版および 64 ビット版 Windows® で使用できます。MPC および VKC は、32 ビット版ブラウザ、64 ビット版 Internet Explorer 7、または 64 ビット版 Internet Explorer 8 からのみ起動できます。

次の表に、Java™ 32 ビットおよび 64 ビット Windows におけるソフトウェア要件を示します。

モード	オペレーティング システム	ブラウザ
Windows x64 32 ビット モード	Windows XP®	• Internet Explorer® 6.0 SP1 以降、IE 7、IE 8 • Firefox® 1.06 ～ 3
	Windows Server 2003®	• Internet Explorer 6.0 SP1 以降、IE 7、IE 8 • Firefox 1.06 ～ 3
	Windows Vista®	• Internet Explorer 7.0 または 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 ～ 3
Windows x64 64 ビット モード	Windows XP	64 ビット OS 対応の 32 ビット版ブラウザ • Internet Explorer 6.0 SP1 以降、7.0、または 8.0 • Firefox 1.06 ～ 3 64 ビット OS 対応の 64 ビット版ブラウザ • Internet Explorer 7.0 または 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

サポートされているブラウザ

LX でサポートされているブラウザは、次のとおりです。

- Internet Explorer® 6 ～ 9
- Firefox® 1.5、2.0、3.0 (ビルド 3.6.17 まで) および 4.0
- Safari® 3 以降

サポートされている CIM とオペレーティング システム

D2CIM に加え、Dominion CIM がサポートされています。次の表に、サポートされているターゲット サーバ オペレーティング システム、CIM、仮想メディア、およびマウス モードを示します。

注: D2CIM-VUSB は、Sun™ (Solaris™) ターゲット サーバではサポートされていません。

サポートされている LX D2CIM	ターゲット サーバおよびリモート ラック PDU	仮想メディア	ずれないマウス モード	インテリジェント マウス モード	標準モード
D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • openSUSE 10、11 • Fedora Core 3 以降 • Mac OS	✓	✓	✓	✓
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓
D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • openSUSE 10、11 • Fedora 8 ～ 11 • Mac OS	✓	✓	✓	✓

サポートされている LX D2CIM	ターゲット サーバおよびリモート ラック PDU	仮想メディア	ずれないマウス モード	インテリジェント マウス モード	標モ
	• Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5	✓		✓	✓

サポートされている画面解像度

各ターゲット サーバの画面解像度とリフレッシュ レートが LX でサポートされているかどうか、および、映像信号がノンインタレース方式であるかどうかを確認してください。

画面解像度とケーブル長は、マウスを同期させるうえで重要な要素です。「*ターゲット サーバとの接続距離および画面解像度* 『*210*p. 』」を参照してください。

LX でサポートされている画面解像度は次のとおりです。

解像度	
640x350、70Hz	1024x768、85Hz
640x350、85Hz	1024x768、75Hz
640x400、56Hz	1024x768、90Hz
640x400、84Hz	1024x768、100Hz
640x400、85Hz	1152x864、60Hz
640x480、60Hz	1152x864、70Hz
640x480、66.6Hz	1152x864、75Hz
640x480、72Hz	1152x864、85Hz
640x480、75Hz	1152x870、75.1Hz
640x480、85Hz	1152x900、66Hz
720x400、70Hz	1152x900、76Hz
720x400、84Hz	1280x720、60Hz

解像度	
720x400、85Hz	1280x960、60Hz
800x600、56Hz	1280x960、85Hz
800x600、60Hz	1280x1024、60Hz
800x600、70Hz	1280x1024、75Hz
800x600、72Hz	1280x1024、85Hz
800x600、75Hz	1360x768、60Hz
800x600、85Hz	1366x768、60Hz
800x600、90Hz	1368x768、60Hz
800x600、100Hz	1400x1050、60Hz
832x624、75.1Hz	1440x900、60Hz
1024x768、60Hz	1600 x 1200、60Hz
1024x768、70Hz	1680x1050、60Hz
1024x768、72Hz	1920x1080、60Hz

ターゲット サーバとの接続距離および画面解像度

ProductName とターゲット サーバの間の最大接続距離は、さまざまな要素によって決まります。たとえば、Cat5 ケーブルのタイプと品質、サーバのタイプと製造元、ビデオ ドライバ、モニタ、環境条件、ユーザの要求レベルなどに左右されます。1600x1200 と 1920x1080 の画面解像度の場合、垂直走査周波数は 60 であり、最大接続距離は 50 フィート (15m) です。

注: サーバの製造メーカーやタイプ、OS のバージョン、ビデオ ドライバなどは多種多様であるうえ、ビデオ品質にはユーザーの主観が反映されるため、Raritan ではあらゆる環境でのすべての距離におけるパフォーマンスを保証することはできません。

LX でサポートされている画面解像度については、「***サポートされている画面解像度*** *『13*p. *』*」を参照してください。

認定モデム

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

リモート接続

リモート接続	詳細情報
ネットワーク	10BASE-T、100BASE-T、および 1000BASE-T (Gigabit) Ethernet
プロトコル	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS、LDAP/LDAPS

各言語に対してサポートされているキーボード

次の表に、各言語に対して LX でサポートされているキーボードを示します。

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。アメリカ英語以外のキーボードの詳細については、「**留意事項** *『226p. 』」を参照してください。*

注: Linux 環境で作業する場合は、system-config-keyboard を使用して言語を変更することをお勧めします。

言語	地域	キーボード レイアウト
US 英語	米国および大半の英語圏の諸国: カナダ、オーストラリア、ニュージーランドなど	US キーボード レイアウト
US インターナショナル	米国および大半の英語圏の諸国: オランダなど	US キーボード レイアウト
UK 英語	英語（イギリス）	UK レイアウト キーボード
繁体字中国語	香港、中国（台湾）	繁体字中国語

言語	地域	キーボード レイアウト
簡体字中国語	中国	簡体字中国語
韓国語	韓国	Dubeolsik ハングル
日本語	日本	JIS キーボード
[French] (フランス語)	フランス	フランス語 (AZERTY) レイアウト キーボード
[German] (ドイツ語)	ドイツおよびオーストリア	ドイツ語キーボード (QWERTZ レイアウト)
[French] (フランス語)	ベルギー	ベルギー語 (ベルギー)
ノルウェー語 (ノルウェー)	ノルウェー	ノルウェー語 (ノルウェー)
デンマーク語 (デンマーク)	デンマーク	デンマーク語 (デンマーク)
スウェーデン語 (スウェーデン)	スウェーデン	スウェーデン語 (スウェーデン)
ハンガリー語	ハンガリー	ハンガリー語
スロベニア語	スロベニア	スロベニア語
イタリア語	イタリア	イタリア語
スペイン語	スペインおよび大半のスペイン語圏の諸国	スペイン語
ポルトガル語	ポルトガル	ポルトガル語

使用される TCP ポートおよび UDP ポート

ポート	説明
HTTP、ポート 80	このポートは、必要に応じて設定できます。「*HTTP ポートおよび HTTPS ポートの設定* 『*133*p. 』」を参照してください。セキュリティを確保するため、デフォルトでは、LX によって HTTP (ポート 80) で受信された要求は、すべて HTTPS に自動変換されます。要求はポート 80 で受け付けられるので、ユーザはブラウザのアドレス ボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも確保されます。
HTTP、ポート 443	このポートは、必要に応じて設定できます。「*HTTP ポートおよび HTTPS ポートの設定* 『*133*p. 』」を参照してください。デフォルトでは、このポートはさまざまな目的で使用されます。たとえば、クライアントから HTML で Web サーバにアクセスする場合、クライアント ソフトウェア (MPC/VKC) をクライアントにダウンロードする場合、KVM データと仮想メディア データをクライアントに転送する場合などです。
LX (Raritan KVM-over-IP) プロトコル、ポート 5000 (変更可)	このポートは、他の Dominion デバイスの検出、および、Raritan デバイスと各種システムとの間の通信に使用されます。このポートはデフォルトで 5000 に設定されていますが、別の TCP ポートに変更することもできます。この設定を変更する手順については、「*ネットワーク設定* 『*128*p. 』」を参照してください。
SNTP (時刻サーバ)、UDP ポート 123 (変更可)	LX の内部クロックを中央の時刻サーバと同期させることができます。この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を使用する必要がありますが、別のポートに変更することもできます。**(オプション)**
LDAP/LDAPS、ポート 389 または 636 (変更可)	LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように LX が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
RADIUS、ポート 1812 (変更可)	RADIUS プロトコルを使用してユーザをリモート認証するように LX が設定されている場合、デフォルトでポート 1812 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
設定可能なポート 1813 を使用する RADIUS アカウンティング	RADIUS プロトコルを使用してユーザをリモート認証するように LX が設定されており、かつ、イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。
SYSLOG、UDP ポート 514 (変更可)	メッセージを Syslog サーバに送信するように LX が設定されている場合、通信にデフォルトでこのポートが使用されます。ただし、別のポ

	ートに変更することもできます。
SNMP、デフォルトの UDP ポート	送受信の読み取り/書き込み SNMP アクセスにはポート 161 が使用されます。SNMP トラップの送信トラフィックにはポート 162 が使用されます。**(オプション)**
TCP ポート 21	ポート 21 は、LX のコマンド ライン インタフェース (CLI) を利用する際に使用されます (お客様が Raritan のテクニカル サポート部門と協力して作業する場合)。

監査ログおよび Syslog でキャプチャされるイベント

LX の監査ログと syslog でキャプチャされるイベントのリストは、次のとおりです。

- システム スタートアップ
- システム シャットダウン
- ネットワーク パラメータ変更
- ポートのステータス変更
- ネットワーク エラー
- 通信エラー
- 出荷時設定にリセット
- デバイス更新開始
- デバイス更新完了
- デバイス更新失敗
- ファームウェア更新失敗
- ファームウェア ファイル破棄
- ファームウェア検証失敗
- 構成バックアップ
- 構成復元
- ポート接続拒否
- アクティブな USB プロファイル
- 証明書更新
- 時刻設定変更
- パスワード設定変更
- ログイン失敗
- パスワード変更
- ユーザ ブロック
- ポート接続
- ポート切断
- アクセス ログイン
- アクセス ログアウト
- 切断
- セッション タイムアウト
- VM イメージ接続
- VM イメージ切断
- CIM 更新開始
- CIM 更新完了
- CIM 接続
- CIM 切断

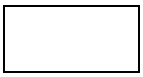
- 重複 CIM シリアル
- ユーザ強制ログアウト
- スキャン開始
- スキャン停止
- ユーザ追加
- ユーザ変更
- ユーザ削除
- グループ追加
- グループ変更
- グループ削除

ネットワーク速度の設定

LX におけるネットワーク速度の設定

ネットワーク スイッチにおけるポートの設定		自動	1000/全二重	100/全二重	100/半二重	10/全二重	10/半二重
	自動	使用可能な最高速度	1000/全二重	LX: 100/全二重 スイッチ: 100/半二重	100/半二重	LX: 10/全二重 スイッチ: 10/半二重	10/半二重
	1000/全二重	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
	100/全二重	LX: 100/半二重 スイッチ: 100/全二重	LX: 100/半二重 スイッチ: 100/全二重	100/全二重	LX: 100/半二重 スイッチ: 100/全二重	通信不可	通信不可
	100/半二重	100/半二重	100/半二重	LX: 100/全二重 スイッチ: 100/半二重	100/半二重	通信不可	通信不可
	10/全二重	LX: 10/半二重 スイッチ: 10/全二重	通信不可	通信不可	通信不可	10/全二重	LX: 10/半二重 スイッチ: 10/全二重
	10/半二重	10/半二重	通信不可	通信不可	通信不可	LX: 10/全二重 スイッチ: 10/半二重	10/半二重

凡例:


通信できません。


サポートされています。

通信は行えますが、推奨できません。


Ethernet 仕様でサポートされていません。通信は行えますが、衝突が発生します。


Ethernet 仕様では通信できないことになっています。LX は期待どおりに動作しません。

注: ネットワーク通信の信頼性を高めるため、LX とネットワーク スイッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえば、LX とネットワーク スイッチの双方で "自動検出" に設定するか (推奨)、または、双方の通信速度と通信速度を同じ設定にします (例: 100 Mbps/全二重)。

Ap B LDAP スキーマを更新する

注: この章で説明する手順は、経験豊富なユーザだけが実行してください。

この章の内容

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、LX では、そのユーザの所属グループに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような属性が返されるので、ユーザ グループ名がわかります。

rciusergroup attribute type: string

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

注: この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000® オペレーティング システム サーバ 上の Microsoft® Active Directory からユーザ グループ情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

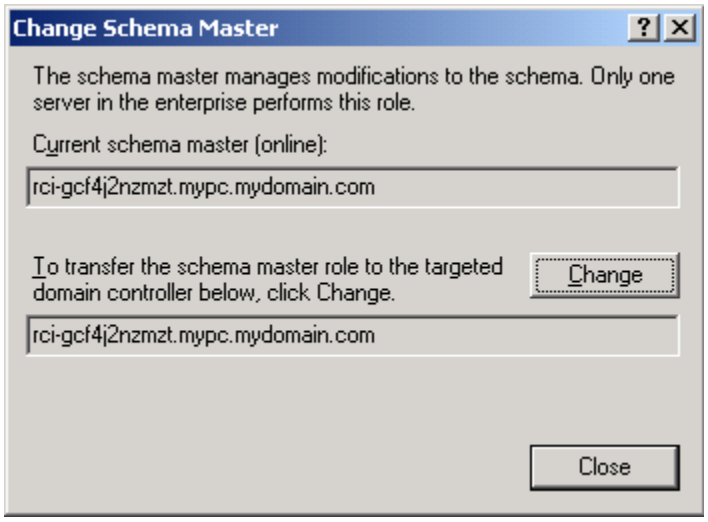
1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



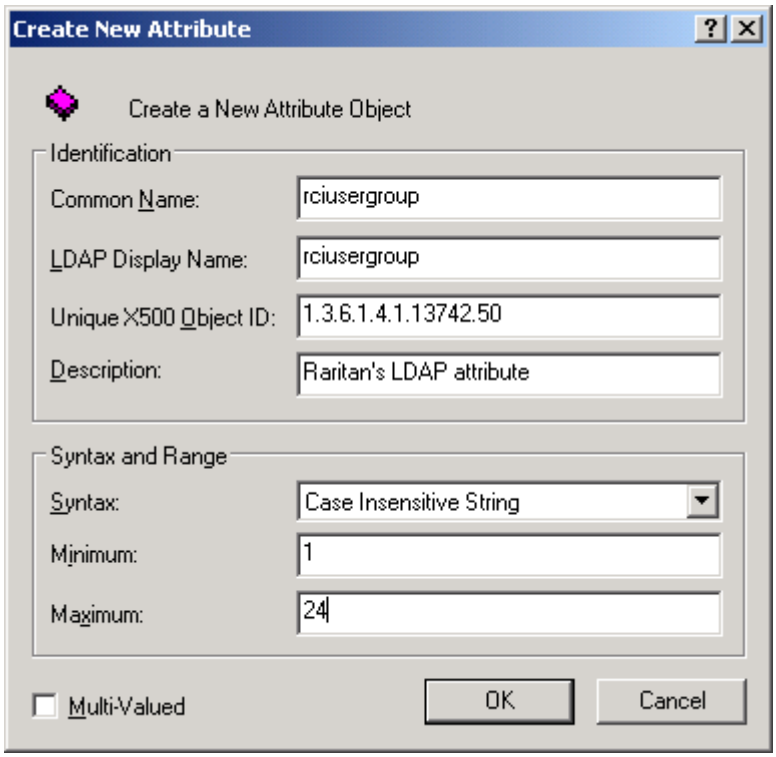
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**

3. [OK] (OK) をクリックします。

新しい属性を作成する

rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。
3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。



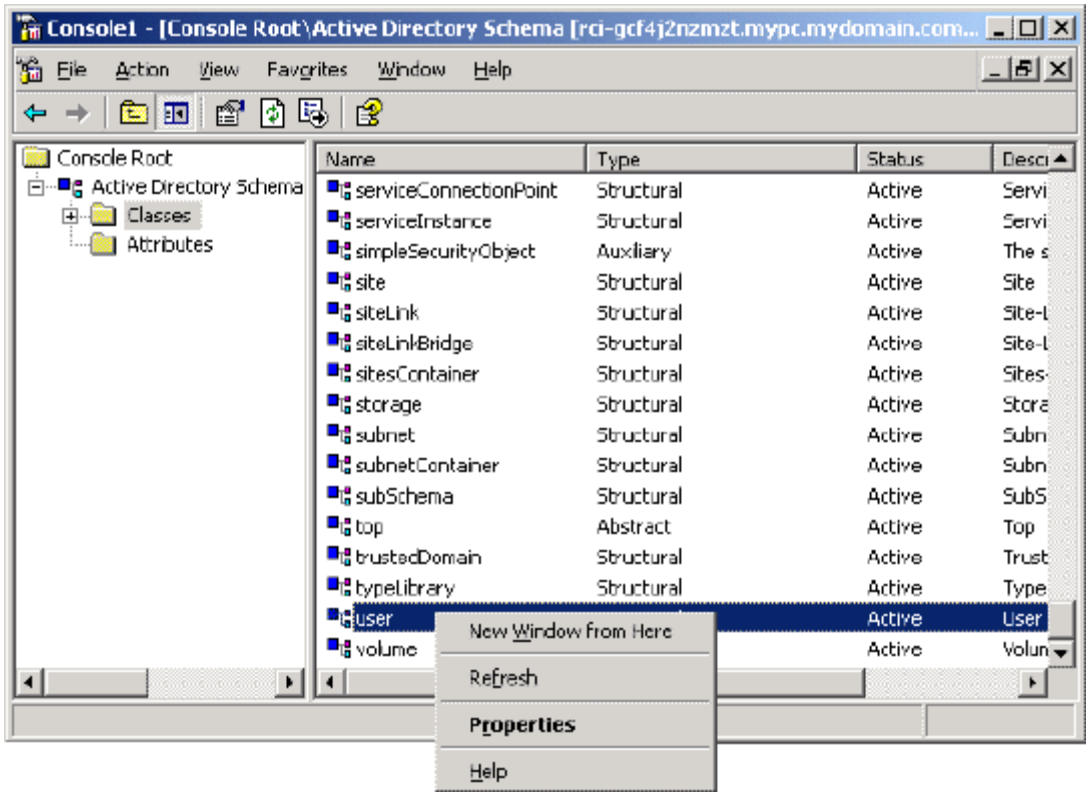
4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。

9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

▶ 属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。
2. 右ペインをスクロールして [user] (user) を表示し、右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。

7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

スキーマ キャッシュを更新するには

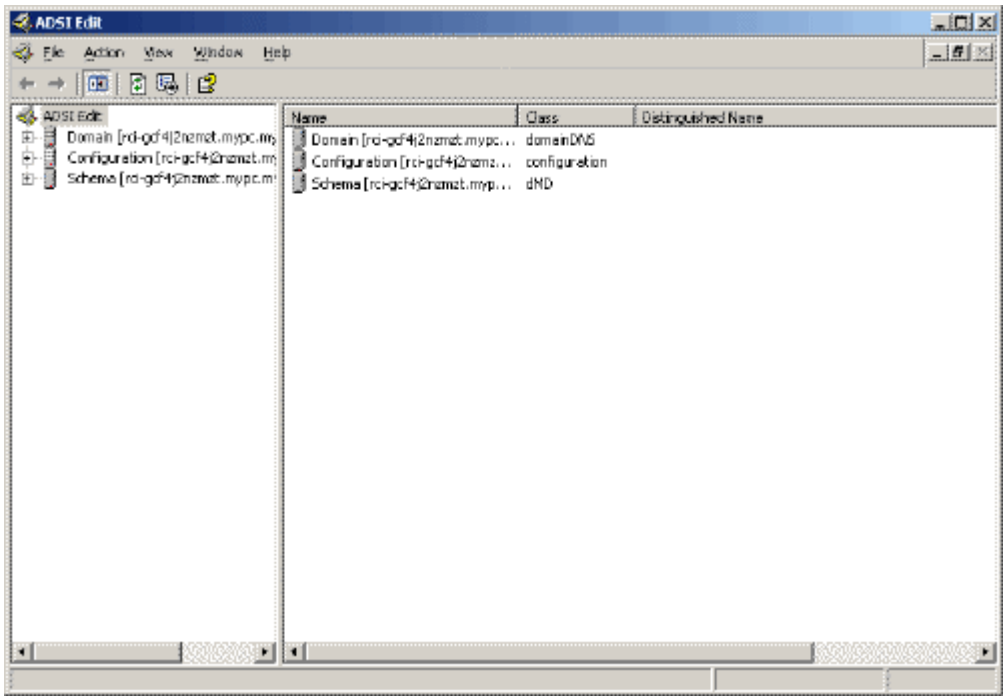
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003® 上で Active Directory® スクリプトを実行するには、Microsoft® から提供されるスクリプトを使用します (Windows Server 2003 のインストール用 CD-ROM に収録されています)。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

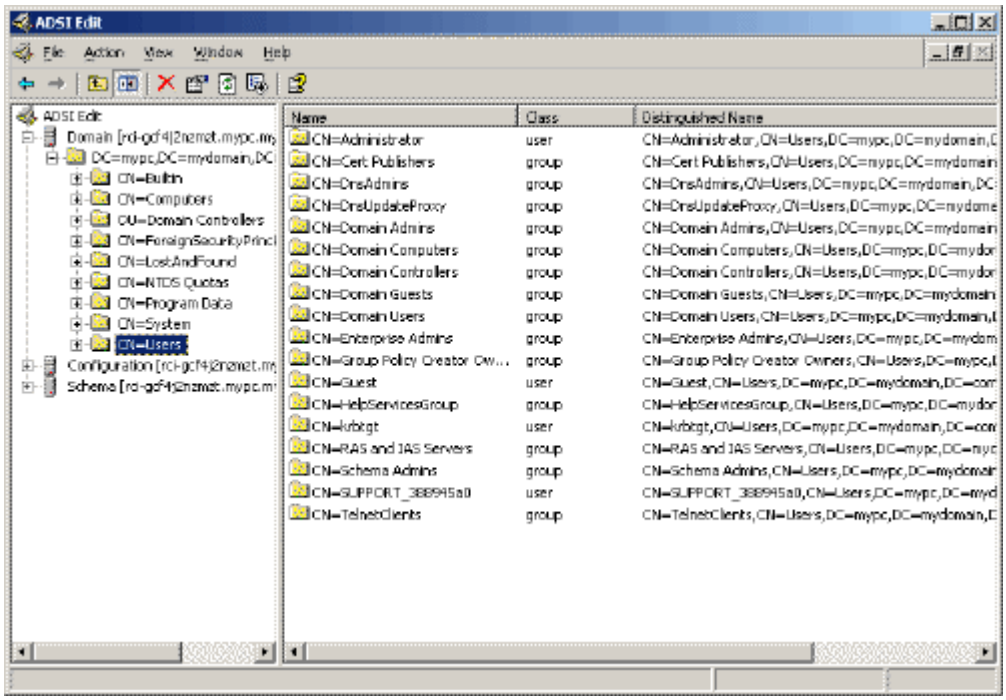
rciusergroup グループ内の個別のユーザ属性を編集するには、以下の手順に従います。

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。



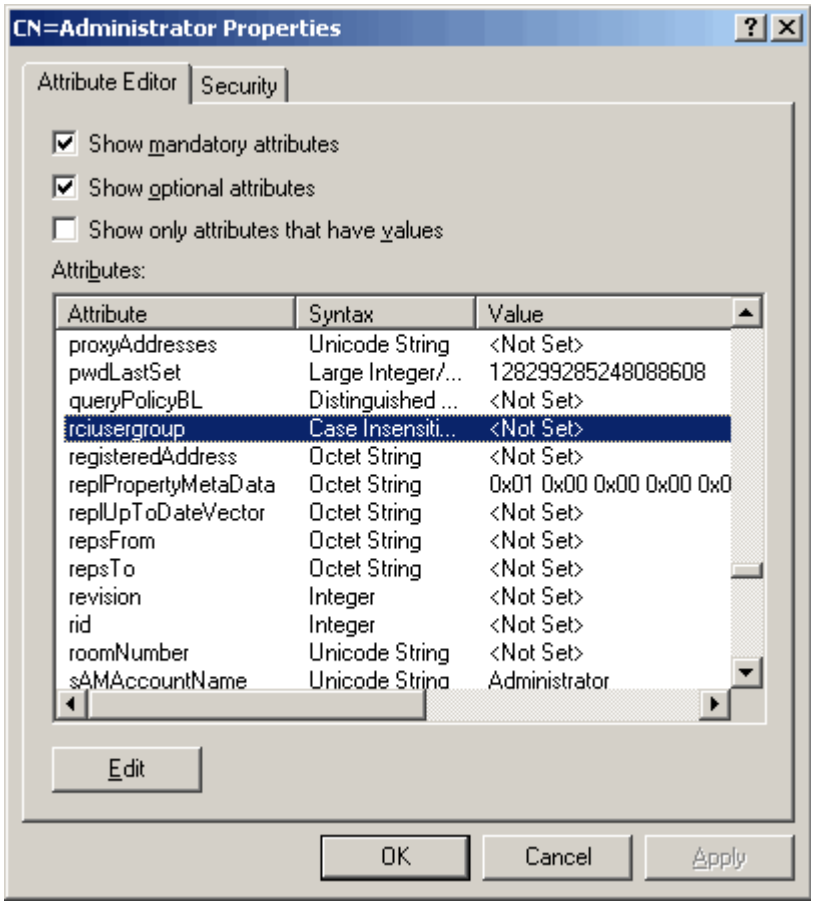
4. [Domain] (ドメイン) を開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

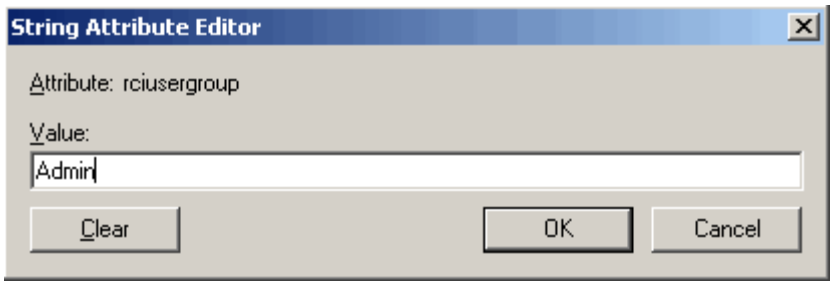


6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューの [Properties] (プロパティ) をクリックします。

7. [Attribute Editor]（属性エディタ）タブをクリックします。[Attributes]（属性）ボックスの一覧で [rciusergroup]（rciusergroup）を選択します。



8. [Edit]（編集）をクリックします。[String Attribute Editor]（文字列属性エディタ）ダイアログ ボックスが開きます。
9. [Value]（値）ボックスに、LX で作成したユーザ グループを入力します。[OK] をクリックします。



Ap C 留意事項

この章の内容

概要

この章では、LX の使用に関する重要事項について説明します。今後更新される情報については、弊社 Web サイトで提供されます。更新情報を表示するには、LX リモート コンソールの [Help] (ヘルプ) リンクをクリックしてください。

注: このセクションの一部のトピックでは、記載されている情報がさまざまなデバイスに影響を与えるため、他の複数の Raritan デバイスにも言及しています。

Java Runtime Environment (JRE)

重要: Java のキャッシュ機能を無効にし、Java™ キャッシュをクリアすることをお勧めします。詳細については、Java のドキュメントまたは『KVM and Serial Access Clients Guide』を参照してください。

LX、KX II、KX II-101、および KX II-101-V2 リモート コンソールおよび MPC では、リモート コンソールで Java のバージョンをチェックするので、実行に Java Runtime Environment™ (JRE™) が必要です。バージョンが不適切であるかまたは古い場合、互換性のあるバージョンをダウンロードするよう指示されます。

パフォーマンスを最大化するため、JRE バージョン 1.6 を使用することをお勧めします。ただし、リモート コンソールおよび MPC は、JRE バージョン 1.6.x 以降 (1.6.2 を除く) でも動作します。

注: 多言語対応のキーボードを LX、KX II、KX II-101、および KX II-101-V2 リモート コンソール (Virtual KVM Client (VKC)) で使用できるようにするには、多言語バージョンの JRE をインストールする必要があります。

IPv6 のサポートに関する注意事項

Java

Java™ 1.6 では、次のオペレーティング システム（OS）に対して IPv6 がサポートされています。

- Solaris™ 10 以降
- Linux® カーネル 2.1.2 以降/RedHat 6.1 以降

Java 5.0 以降では、次の OS に対して IPv6 がサポートされています。

- Solaris 10 以降
- Linux カーネル 2.1.2 以降（IPv6 対応に優れた 2.4.0 以降を推奨）
- Windows XP® SP1、Windows 2003®、および Windows Vista®

Java では、次の IPv6 構成は*サポートされていません*。

- Microsoft® Windows® 上の J2SE 1.4 では、IPv6 はサポートされていません。

Linux

- IPv6 を使用する場合、Linux カーネル 2.4.0 以降を使用することをお勧めします。
- IPv6 対応のカーネルをインストールするか、または、IPv6 関連オプションを有効にしてカーネルを再ビルドする必要があります。
- IPv6 を使用する場合、Linux 用のネットワーク ユーティリティをいくつかインストールする必要があります。詳細については、http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html を参照してください。

Windows

- Windows XP ユーザまたは Windows 2003 を使用している場合、Microsoft の IPv6 対応サービス パックをインストールし、IPv6 を有効にする必要があります。

Mac Leopard

- KX II version 2.0.20 では、Mac® Leopard® に対して IPv6 はサポートされていません。

Samba

- Samba を使用する場合、IPv6 と仮想メディアを併用することはできません。

キーボード

アメリカ英語以外のキーボード

フランス語キーボード

キャレット記号 (Linux® クライアントのみ)

Linux クライアントとフランス語キーボードを併用する場合、VKC および MPC では Alt Gr + 9 というキー組み合わせがキャレット記号（ˆ）として処理されません。

▶ キャレット記号を入力するには

フランス語キーボードの ^ キー（P キーの右にある）を押し、すぐに Space キーを押します。

次のコマンドを実行するマクロを作成する方法もあります。

1. 右 Alt キーを押す。
2. 9 キーを押す。
3. 9 キーを離す。
4. 右 Alt キーを離す。

注: これらの手順は、母音の上に付ける曲折アクセントには当てはまりません。フランス語キーボードで ^ キーと他の文字を組み合わせて使用した場合、曲折アクセントになります。

アクセント記号 (Windows XP® クライアントのみ)

Windows XP クライアントでフランス語キーボードを使用する場合、VKC および MPC で Alt Gr + 7 というキー組み合わせを使用すると、アクセント記号付き文字が 2 つ表示されます。

注: この現象は、Linux クライアントでは発生しません。

数字キーパッド

VKC および MPC でフランス語キーボードを使用する場合、数字キーパッドにある記号は次のとおりに表示されます。

数字キーパッド上の記号キー	表示
/	;
.	;

ティルデ記号

VKC および MPC でフランス語キーボードを使用する場合、Alt Gr + 2 というキー組み合わせがティルデ記号（~）として処理されません。

▶ ティルデ記号を入力するには

次のコマンドを実行するマクロを作成します。

- 右 Alt キーを押す。
- 2 キーを押す。
- 2 キーを離す。
- 右 Alt キーを離す。

キーボード言語の設定 (Fedora クライアント)

Linux® 版の JRE™ には、[System Preferences]（システム基本設定）で設定した外国語キーボードに対して正しいキー イベントが生成されない、という問題があります。したがって、次の表に示す方法を使用して外国語キーボードを設定することを推奨します。

言語	設定方法
アメリカ英語/国際	デフォルト設定
イギリス英語	[System Settings]（システム設定）(Control Center)
フランス語	Keyboard Indicator
ドイツ語	Keyboard Indicator
ハンガリー語	[System Settings]（システム設定）(Control Center)
スペイン語	[System Settings]（システム設定）(Control Center)
ドイツ語（スイス）	[System Settings]（システム設定）(Control Center)
ノルウェー語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
デンマーク語	Keyboard Indicator
日本語	[System Settings]（システム設定）(Control Center)
韓国語	[System Settings]（システム設定）(Control

言語	設定方法
アメリカ英語/国際	デフォルト設定
	Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

Linux クライアントでハンガリー語キーボードを使用している場合、ダブル アキュート付き U およびダブル アキュート付き O は、JRE 1.6 でのみ入力できます。

Fedora® クライアントでは、キーボード言語を設定する方法がいくつかあります。VKC および MPC でキーを正しく対応付けるには、次に示す方法を使用します。

[System Settings] (システム設定) を使用してキーボード言語を設定するには

1. ツールバーで [System] (システム) > [Preferences] (基本設定) > [Keyboard] (キーボード) を選択します。
2. [Layouts] (レイアウト) タブをクリックします。
3. 言語を追加または選択します。
4. [Close] (閉じる) をクリックします。

Keyboard Indicator を使用してキーボード言語を設定するには

1. タスク バーを右クリックし、[Add to Panel] (パネルに追加) をクリックします。
2. [Add to Panel] (パネルに追加) ダイアログ ボックスで、Keyboard Indicator を右クリックし、メニューの [Open Keyboard Preferences] (キーボード基本設定) をクリックします。
3. [Keyboard Preferences] (キーボード基本設定) ダイアログ ボックスで、[Layouts] (レイアウト) タブをクリックします。
4. 必要に応じて言語を追加または削除します。

Macintosh キーボード

クライアントとして Macintosh® を使用している場合、Macintosh キーボードの次のキーは、JRE™ によって取り込まれません。

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

つまり、Macintosh クライアントのキーボードでこれらのキーが押されても、VKC および MPC では処理できません。

Fedora

Fedora Core のフォーカスに関する問題を解決する

MPC を使用しているときに、LX、KX II、または KSX II デバイスにログインできなくなったり、Windows® や SUSE を実行している KVM ターゲット サーバにアクセスできなくなったりすることがあります。また、Ctrl + Alt + M キーを押してもキーボード ショートカット メニューが表示されないことがあります。このような問題が発生するのは、Fedora® Core 6 と Firefox® 1.5 または 2.0 を組み合わせて使用している場合です。

Raritan でテストした結果、libXp をインストールすれば Fedora Core 6 のウィンドウ フォーカスに関する問題を解決できることがわかりました。Raritan がテストで使用したのは libXp-1.0.0.8.i386.rpm です。この libXp をインストールした結果、ウィンドウ フォーカスとポップアップ メニューに関する問題がすべて解決しました。

注: libXp は、SeaMonkey (旧称: Mozilla®) ブラウザで Java™ プラグインを使用する場合にも必要となります。

マウス ポインタの同期 (Fedora)

Fedora® 7 を実行しているターゲット サーバにデュアル マウス モードで接続しているときに、ターゲット サーバとローカルのマウス ポインタが同期しなくなった場合、マウス モードをインテリジェント モードに、またはインテリジェント モードから標準モードに変更すると同期が回復することがあります。シングル マウス モードを使用すると、制御しやすくなります。

▶ **マウス ポインタを再度同期させるには、以下の手順に従います。**

- VKC の [Synchronize Mouse] (マウスを同期) オプションを使用します。

Fedora 使用時の Firefox のフリーズに関する問題の解決

Fedora® サーバを使用している場合に Firefox® にアクセスすると、Firefox を開くときに Firefox がフリーズすることがあります。この問題を解決するには、libnpjp2.so という Java™ プラグインをサーバにインストールします。

ビデオ モードと解像度

SUSE と VESA のビデオ モード

SUSE の X.org 設定ツールである SaX2 を実行すると、X.org 設定ファイル内の Monitor セクションの Modeline エントリにビデオ モードが書き込まれます。これらのビデオ モードは、VESA モニタを選択している場合であっても、VESA のビデオ モード タイミングと正確に対応していません。一方 LX では、正確に同期させるため、VESA のビデオ モード タイミングが使用されています。このビデオ モード タイミングの不一致により、黒の境界線が表示される、画面の一部が表示されない、ノイズが発生する、などの問題が発生することがあります。

▶ **SUSE のビデオ表示を設定するには**

1. 生成された設定ファイル /etc/X11/xorg.conf 内に Monitor セクションがあり、その中に UseModes というオプションがあります。たとえば、
   UseModes "Modes[0]" と書き込まれています。
2. この行の先頭に # を付加してコメント行にするか、または、この行全体を削除します。
3. X サーバを再起動します。

これにより、X サーバの内部ビデオ モード タイミングが使用されるようになるので、VESA のビデオ モード タイミングと正確に対応します。この結果、LX 経由で画面が正しく表示されます。

サポートされている画面解像度が表示されない

CIM を使用する場合、「サポートされている画面解像度」の一覧にある画面解像度がデフォルトでは選択できないことがあります。

▶ **表示されない場合に利用可能なすべての画面解像度を表示するには、以下の手順に従います。**

1. モニタを接続します。
2. 次に、モニタを取り外し、CIM を接続します。すべての画面解像度が利用可能とは限りませんが、使用できる場合もあります。

VM-CIM および DL360 の USB ポート

HP® DL360 サーバの背面と前面には、USB ポートがそれぞれ 1 つあります。DL360 では、両方の USB ポートを同時に使用することはできません。つまり、DL360 サーバに対してデュアル VM-CIM を使用することはできません。

ただし、代替策として、DL360 サーバの背面の USB ポートに USB2 ハブを接続し、そのハブにデュアル VM-CIM を接続することはできます。

MCUTP

MCUTP に設定されているシリアル番号と CIM 名は、デバイスに保存されません。このように、MCUTP ポートは他のポートと異なった動作になります。次に例を示します。

- CIM には名前のストレージがなく、ポートにはさまざまな CIM タイプが接続されるため、ポート タイプが変更されない間は、ポート名がラベルとしてポートに関連付けられる。
- 電源の関連付けは、このタイプのポートには作成できない。
- ターゲット設定は、このタイプのポートには適用できない。
- シリアル番号は、CIM シリアル番号を表示する画面やログ エントリでは「なし」と表示される。
- このタイプのポートをポート グループに関連付けることはできない。
- このタイプのポートを接続スクリプトに関連付けることはできない。

仮想メディア

Windows 環境での VKC および AKC を介した仮想メディア

Windows XP® の Administrator 権限および標準ユーザ権限は、Windows Vista® および Windows 7® とは異なります。

Vista または Windows 7 でユーザ アクセス制御（UAC）を有効にすると、ユーザがアプリケーションの実行に必要とする最低レベルの権限が与えられます。たとえば、Internet Explorer® でユーザに管理者レベルのタスクの実行を明示的に許可するための［管理者として実行］オプションが用意されています。このオプションを使用しない場合、ユーザは管理者としてログインしていても管理者レベルのタスクを実行できません。

これらの両方の機能は、ユーザが Virtual KVM Client（VKC）および Active KVM Client（AKC）を使用してアクセスできる仮想メディアのタイプに影響します。これらの機能の詳細および使用方法については、Microsoft® のヘルプを参照してください。

ユーザが Windows 環境で VKC および AKC を使用してアクセスできる仮想メディアのタイプを以下に示します。機能をクライアント別に分類し、各 Windows ユーザ役割がアクセスできる仮想メディア機能を示します。

Windows XP

VKC および AKC を Windows XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Windows Vista および Windows 7

VKC および AKC を Windows Vista または Windows 7 環境で実行し、UAC が有効になっている場合は、ユーザの Windows 役割に応じて以下の仮想メディア タイプにアクセスできます。

クライアント	管理者	標準ユーザ
AKC および VKC	アクセス先: • 固定ドライブと固定ドライブ パーティション • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ	アクセス先: • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ

ドライブ パーティション

- オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。
  - Windows および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
  - Windows® および Linux® では Mac 形式のパーティションの読み取りはできない
  - Linux でサポートされているのは Windows Fat パーティションのみ
  - Windows FAT および NTFS は Mac でサポートされている

  Mac ユーザがターゲットサーバに接続するためには、既にマウントされているデバイスをアンマウントする必要があります。デバイスをアンマウントするには、>diskutil umount /dev/disk1s1 を使用し、再マウントするには、diskutil mount /dev/disk1s1 を使用します。

ファイル追加後に仮想メディアが最新の情報に更新されない

仮想メディア ドライブがマウントされた後、そのドライブにファイルを追加した場合、ターゲット サーバ側でそのファイルがすぐに表示されないことがあります。表示するには、仮想メディア接続をいったん解除し、再確立します。

アクティブ システム パーティション

Mac または Linux クライアントからアクティブ システム パーティションをマウントすることはできません。

Linux Ext3/4 ドライブ パーティションは、仮想メディアを接続する前に umount /dev/<device label> でアンマウントしておく必要があります。

ドライブ パーティション

オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。

- Windows および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
- Windows® および Linux® では Mac 形式のパーティションの読み取りはできない
- Linux でサポートされているのは Windows Fat パーティションのみ
- Windows FAT および NTFS は Mac でサポートされている

- Mac ユーザがターゲットサーバに接続するためには、既にマウントされているデバイスをアンマウントする必要があります。デバイスをアンマウントするには、>diskutil umount /dev/disk1s1 を使用し、再マウントするには、diskutil mount /dev/disk1s1 を使用します。

仮想メディアの Linux ドライブが 2 回リストされる

KX II 2.4.0 以降および LX 2.4.5 以降では、ユーザが Linux™ クライアントに root ユーザとしログインしている場合、ドライブが［ローカル ドライブ］ドロップダウン リストに 2 回リストされます。たとえば、eg /dev/sdc と eg /dev/sdc1 が表示されます。1 つ目のドライブはブートセクタ、2 つ目のドライブはディスクの最初のパーティションです。

Mac および Linux でマップしてロックしたドライブ

Mac® および Linux® クライアントからマップされたドライブは、接続されたターゲットにマウントされた場合にロックされません。これは、Mac および Linux のサポートを提供する KX II 2.4.0 以降および LX 2.4.5 以降にのみ該当します。

D2CIM-VUSB を使用して Windows 2000 サーバ上の仮想メディアにアクセスする

D2CIM-VUSB を使用して Windows 2000® サーバ上の仮想メディアに仮想メディア ローカル ドライブにアクセスすることはできません。

仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間

ターゲット サーバにおいてメディアが仮想マウントされている場合、そのターゲット サーバの BIOS の起動に要する時間が長くなることがあります。

起動に要する時間を短縮するには

1. VKC を終了し、仮想メディア ドライブを完全に解放します。
2. ターゲット サーバを再起動します。

高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー

［高速 USB］接続でターゲットに問題が発生する場合、またはターゲットで接続やケーブルの追加（たとえば、ドングルを使用したブレード サーバへの接続）に起因する信号劣化により USB プロトコル エラーが発生する場合は、［仮想メディア CIM でフル スピードを使用］の選択が必要になることがあります。.

CIM

Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合

Linux® ターゲット サーバに接続している Windows® クライアントで 3 ボタン マウスを使用する場合、左マウス ボタンがその 3 ボタン マウスの中央ボタンに対応付けられることがあります。

Windows 2000 での複合 USB デバイスの動作

Windows 2000® では、Raritan の D2CIM-VUSB のような複合 USB デバイスはサポートされていないので、非複合 USB デバイスと同じように扱われます。

したがって、D2CIM-VUSB によってマッピングされているドライブに対する［ハードウェアの安全な取り外し］アイコンがシステム トレイに表示されません。また、D2CIM-VUSB を取り外す際、警告メッセージが表示されることがあります。Raritan が確認したところでは、このメッセージが表示されても何の問題も発生しません。

MCUTP CIM の動作

MCUTP に設定されている CIM シリアル番号や CIM 名のストレージがないので、このタイプのポートは、特に、以下の点において他の CIMS と異なった動作になります。

- CIM 名が格納されない。
- ポートにはさまざまな CIM タイプが接続されるため、ポート タイプが変更されない間は、ポート名がラベルとしてポートに関連付けられる。
- ターゲット設定は、このタイプのポートには適用できない。
- シリアル番号は、CIM シリアル番号を表示する画面やログ エントリでは「なし」と表示される。

Ap D FAQ

この章の内容

Ch 12

LX FAQ

質問	回答
Dominion LX とは何ですか?	Dominion LX とは、単一電源、単一 LAN、および仮想メディアを装備している経済的な KVM-over-IP スイッチ ファミリのことです。管理するサーバが 75 台未満の中小企業を対象にしており、1、2 名のリモートユーザによって BIOS レベルで 8 台または 16 台のサーバを IP 制御できます。
LX の代表的なお客様について説明していただけますか?	代表的なお客様は、たいていの場合、低価格でフル装備のリモート KVM-over-IP アクセス機能を必要とする、中小企業の IT 管理者またはソフトウェア開発者/テスターです。LX のお客様は、仮想メディア、ずれないマウス™、一般的なリモート/ローカル ユーザ インタフェースなどの生産性を高める機能を求めています。
Dominion LX の何が特別なのでしょうか?	LX を使用すると、フル装備の高品質な KVM-over-IP スイッチを手頃な価格で実現できます。その価格帯の他の製品と異なり、LX は、仮想メディア、ずれないマウス、一般的なブラウザベースのユーザ インタフェースなどの生産性を高める機能をサポートしています。
LX では、どのような IT 機器を管理できますか?	LX では、コンピュータ サーバ、コンピュータ機器、通信装置、ネットワーク デバイスをはじめとする、コンピュータおよびシリアル制御機器を管理できます。
どのようなリモート管理機能がサポートされていますか?	Dominion LX では、信頼性の高い、帯域外のリモート管理を行うことができます。 このリモート管理には、BIOS レベルの KVM-over-IP 制御、リモート仮想メディア、オプションのモデム アクセスなどがあります。 LX を使用すると、ターゲット デバイスの状態に関係なく、いつでも、どこでもリモート管理を行うことができます。BIOS レベルでの入力、ハードウェア診断の実行、ハングしたサーバの再起動、DVD からのソフトウェアのインストール、およびサーバのイメージの再作成をすべてリモートから行うことができます。
Dominion LX は競合他社製品と比べてどうですか?	一般に競合他社製品は、機能が限られた保守的な OSD ユーザ インタフェースを装備する、エントリレベルの KVM-over-IP スイッチです。競合他社製品には、仮想メディア、ずれないマウス、1920x1080 リモート画面解像度、標準のセキュリティ機能などの標準的な機能が不足しています。

質問	回答
LX では、どのような価値を提供できますか?	中小企業の IT スタッフや開発スタッフ向けの低価格で高品質の KVM-over-IP スイッチを提供できます。 LX では、時間と場所を問わない、サーバやその他の IT デバイスのリモート アクセスおよびリモート制御に基づく価値が提供されます。 LX のお客様は、以下のメリットが得られます。 • 出張旅費の削減 • 生産性の向上 • 平均修理時間の短縮 • より高品質なサービス
技術的な質問	
使用可能な LX モデルはどれですか?	Dominion LX ファミリには、3 つの KVM-over-IP モデルがあります。DLX-108 は、1 リモート ユーザ セッションと 1 ローカル ユーザをサポートする 8 ポート スイッチです。DLX-116 は、1 リモート ユーザ セッションと 1 ローカル ユーザをサポートする 16 ポート スイッチです。DLX-216 は、2 リモート ユーザ セッションと 1 ローカル ユーザをサポートする 16 ポート スイッチです。
ハードウェアにはどのような特徴がありますか?	Dominion LX は、8 または 16 サーバ ポートを搭載した 1U サイズのコンパクトなケース、単一電源、単一ギガビット LAN、オプションのモデム アクセスを備えた USB ベースのローカル ポートを装備しています。
Dominion LX は Dominion KX II と比べてどうですか?	Dominion KX II は、Raritan の最上位に位置するエンタープライズクラスのセキュア KVM-over-IP スイッチです。KX II は、最大 64 台のリモート サーバと最大 8 人のリモート ユーザをサポートするモデルを揃えており、数百台から数千台のサーバを管理する大企業や中企業のお客様を対象にしています。Dominion KX II は、業界で最も信頼性の高いセキュア スイッチであり、二重化電源、二重化 LAN、FIPS 140-2 暗号化モジュール、およびスマート カード/CAC 認証を特徴としています。 Dominion LX は、管理するサーバが 75 台未満の中小企業を対象にした経済的な KVM-over-IP スイッチ ファミリです。LX を使用すると、1、2 名のリモート ユーザによって BIOS レベルで 8 台または 16 台のサーバを IP 制御できます。

質問	回答
Dominion LX の標準的な機能には何がありますか?	Dominion LX の標準的な機能は、次のとおりです。 • 仮想メディア • ずれないマウス • 一般的なブラウザーベースのリモート/ローカル ユーザ インタフェース • 1920x1080 リモート画面解像度 • ローカル認証とリモート認証 (LDAP/AD/RADIUS) • ポート権限と管理者権限 • デュアル スタック IPv6/IPv4 • ポート スキャンとサムネイル表示 • 他の LX スイッチとのカスケード接続 • モデム アクセス • 基本的なセキュリティ機能 詳細については、『**Dominion LX Features and Benefits (Dominion LX の特徴と利点)**』を参照してください。
KX II の機能のうち LX で利用できないのはどれですか?	KX II の機能のうち LX で利用できないものは、次のとおりです。 • CommandCenter® Secure Gateway (CC-SG) 集中管理 • iPad® や iPhone® によるモバイル アクセス (CC-SG が必要) • ブレード サーバ サポート • IP ネットワーク経由のデジタル音声 • FIPS 140-2 暗号化モジュール • スマート カード/CAC サポート • セキュア ログイン バナー • 統合リモート電源管理 • デュアル モニタ オプションと KVM クライアント起動オプション
LX では、どの CIM (サーバ ドングル) を使用できますか?	Dominion LX では、(1) 標準の Dominion CIM と仮想メディア Dominion CIM、(2) 経済的な MCUTP ケーブル CIM、および (3) P2CIM-SER シリアル CIM を使用できます。
MCUTP ケーブル CIM とはどのようなもので、なぜ私にはこれが必要なのですか?	仮想メディアやずれないマウス機能を使用するつもりのないお客様には、MCUTP ケーブル CIM が Dominion CIM に代わる経済的な製品となります。ケーブル CIM とは、さまざまな長さで利用できる Cat5 ケーブルを備えた統合 CIM のことです。
Dominion LX で集中管理はできますか?	Dominion LX の標準の機能では集中管理はできません。

質問	回答
仮想メディアとは何ですか?	仮想メディアとは、KVM 接続中にユーザのデスクトップからリモート サーバにドライブやメディアをマウントできるようになる強力な機能のことです。この機能は、ソフトウェアのインストール、ハードウェア診断の実行、ファイルの転送、およびリモートからのサーバのイメージの再作成などを行う場合に最適です。
Dominion LX では、どのタイプの仮想メディアがサポートされていますか?	Dominion LX でサポートされている仮想メディアのタイプは、内蔵または USB 接続の CD/DVD ドライブ、USB 接続の大容量ストレージ デバイス、PC の内蔵ハード ディスク、およびローカル/リモート ISO イメージです。
ずれないマウスとは何ですか?	これは、Raritan が開発したテクノロジであり、何も設定しなくてもローカルのマウス カーソルとリモートのマウス カーソルが正しく同期する機能です。この機能により、各ターゲット サーバ上で手動でマウス設定を変更する手間が省けます。

索引

H

I

J

K

L

M

N

R

S

U

V

W

あ

か

さ

た

な

は

ま

や

ら

漢字

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 : +44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : rg-support@raritan.com

メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール : support.apac@raritan.com